United Nations A/HRC/35/22/Add.4

General Assembly

Distr.: General
22 May 2017

English only

Human Rights Council
Thirty-fifth session
6-23 June 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression

Addendum

Supplementary Materials Accompanying Annual Report A/HRC/35/22*

* The present document is being circulated in English only, as it exceeds the word limitations currently imposed by the relevant General Assembly resolutions.

GE.17-08194(E)

Please recycle

Contents

		Page
I.	Introduction	3
II.	On the Human Rights Impact of Standards Developing Organizations	3
	A. Standards Developing Organizations	4
	B. Incorporating Human Rights Considerations into Standards Development	9
III.	Overview of Submissions Received in Preparation of A/HRC/35/22	11
	A. The Provision of Internet and Telecommunications Access: Freedom of Expression Issues and Concerns	11
	B. The Human Rights Responsibilities of the Digital Access Sector	15
III.	Summary of Multi-Stakeholder Consultation on Human Rights Due Diligence and the Digital Access Industry	18
	A. Session 1: Identifying Human Rights Risks	19
	B. Session 2: Due Diligence Practices and Procedures	20
	C. Session 3: Remedies	23
	D. Session 4: Transparency	25

I. Introduction

1. This annex accompanies the June 2017 report to the Human Rights Council of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression (A/HRC/35/22). The main report examines the role of State and non-State actors in the provision of Internet and telecommunications access (or "digital access") and their human rights obligations and responsibilities respectively. The report provides guidance concerning the responsibility of digital access providers to respect freedom of expression online.

2. Part II of the Annex discusses the **human rights impact of Standards Developing Organization ("SDOs").** The report explains that SDOs, while not strictly "industry actors", nevertheless "establish technical protocols and standards that enable inter-operability in the telecommunications and Internet infrastructure" (A/HRC/35/22). Part II thus explores the work and governance of major SDOs, their impact on freedom of expression, and the need to incorporate human rights due diligence into standards development.

3. Part III provides an overview of **the submissions that the Special Rapporteur received** from States, civil society organizations, companies, academics and others. Given space limitations, the main report could not discuss these submissions in detail. Part III thus highlights issues and concerns raised in these submissions and other resources that interested readers may wish to investigate.

4. Part IV provides a summary of a **multi-stakeholder consultation on human rights due diligence and the digital access industry** conducted in preparation of the report. The consultation was held on 24 October 2016 and hosted by the University of Connecticut, one of several meetings that helped inform the report.

5. The Special Rapporteur would like to thank the following for their invaluable assistance in preparing this annex: Calvin Bryne, Sarah Choi, and Adam Lhedmat of the International Justice Clinic at the University of California ("UC"), Irvine, who helped research and draft Parts II and III; Molly Land, Fatimah Belem, Katharina Braun, Dorothy Diaz-Hennessey, Richard Hine, and Komla Matrevi of the University of Connecticut, and Katherine Ells of UC Irvine, who helped compile Part IV; and Amos Toh, who coordinated and edited the annex.

6. This annex should be read as a companion to A/HRC/35/22 and does not intend to endorse or reject any of the input provided during the preparation of the report.

II. On the Human Rights Impact of Standards Developing Organizations

7. The Special Rapporteur has identified the development of technical standards as a critical area of human rights discourse (A/HRC/35/22; paras. 43-44; A/HRC/32/38, paras. 27-29). The capacity to seek, receive and impart information online relies on an ever-expanding series of standards and protocols that enable the smooth functioning of Internet and telecommunications networks. The TCP/IP protocols, for example, determine how information should be formatted, addressed and routed among devices within a network and between networks.[1]

[1] See "Transmission Control Protocol/Internet Protocol (TCP/IP)," Techopedia *available at* https://www.techopedia.com/definition/2460/transmission-control-protocolinternet-protocol-tcpip.

A. Standards Developing Organizations

8. Internet and telecommunications standards are developed by a wide variety of Standards Developing Organizations ("SDOs"). Some of these SDOs are loosely governed, composed of volunteers and open to anyone to join, while others have more formal membership structures with varying levels of participation. Many of them attract significant participation from the private sector, while academic and other civil society participation is also common. Major SDOs include:

i. Internet Engineering Task Force ("IETF")

9. *What they do:* Most commonly known for its role in developing the first iteration of the Interne IETF's primary mission is to develop Internet standards. In particular, it "[p]lays a crucial role in managing the logical layer of the Internet, and in designing the standards and protocols that define how information flows across the networks."[2]

10. *Governance:* IETF has no official membership, and its activities are open to anyone.[3] However, many of those involved in drafting standards and the organization's governance are affiliated with the private sector.[4] IETF is organized into seven areas of work: Applications and Real-Time Area (focused on Internet applications protocols and architectures), Internet Area (IP layer protocols), Operations and Management Area (network management), Security Area (security protocols), Routing Area (protocols ensuring continuous operation of the Internet routing system), Transport Area (data transport protocols), and General Area (supporting, updating and maintaining the standards development process).[5] Each Area is managed by one or two Area Directors, who ensure that the "Area is well coordinated, that there is coverage for the technologies needed in the area, and that the challenges most important to the Internet in that area are indeed being worked on."[6] Within each Area, IETF standards are mainly developed through Working Groups ("WGs") and published in documents known as Requests for Comments ("RFCs").[7] Anyone may set up a WG, provided that the advice and consent of the relevant Area Director is obtained and the WG complies with the guidelines and procedures for its formation and operation.[8] Standards are adopted through a consensus-building process that seeks to reflect the "dominant view" of the WG in the event that unanimity cannot be achieved (referred to in the IETF as "rough consensus").[9] WG decisions are frequently made via e-mail on publicly available mailing lists.[10] IETF's three annual meetings also provide an opportunity for WGs to meet and make decisions, and for the organization as a

---

See also DeNardis, Laura, *The Global War for Internet Governance*, Yale University Press (2014) at 67.

[2] ARTICLE 19 submission at 12.

[3] See Internet Society submission at 5; Internet Engineering Task Force, "Getting Started in the IETF" *available at* https://www.ietf.org/newcomers.html.

[4] DeNardis at 66-67, 70.

[5] IETF, "Areas," *available at* https://www.ietf.org/iesg/area.html.

[6] *Id.*

[7] S. Bradner (ed.), Network Working Group, IETF, "IETF Working Group Guidelines and Procedures," RFC 2418 (September 1998), 4, 20, *available at* https://tools.ietf.org/html/rfc2418. The list of active IETF WGs is *available at* https://datatracker.ietf.org/wg/.

[8] RFC 2418 at 4-9.

[9] IETF participants have stressed that "rough consensus" is not majoritarian rule - "51% of the working group does not qualify as "rough consensus" and 99% is better than rough." Consensus is determined not on the "basis of volume or persistence, but rather a more general sense of agreement." RFC 2418 at 13. See also P. Resnick, IETF, "On Consensus and Humming in the IETF," RFC 7282 (June 2014), *available at* https://tools.ietf.org/html/rfc7282 (discussing and critiquing the features of "rough consensus").

[10] ARTICLE 19 submission at 12.

whole to discuss key technical and administrative issues concerning its role in setting Internet standards.[11] During these meetings, consensus is usually determined by humming.[12]

ii. World Wide Web Consortium ("W3C")

11. *What they do:* Another large and well-established SDO, W3C is a membership organization that develops standards and protocols for the World Wide Web, one of the most widely used Internet applications for communication and information exchange (and often synonymous with the Internet for most users).[13] W3C standards include the HyperText Markup Language ("HTML") and Extensible Markup Language ("XML"), the main language responsible for websites. At the time of publication, W3C is considering the adoption of the Encrypted Media Extensions ("EME") specification, which would accommodate the use of Digital Rights Management ("DRM") (software that restricts access to proprietary or copyrighted works) on web browsers.[14] The proposed specification has raised concerns that it will become easier for large media companies to impose onerous restrictions on access to digital content.[15]

12. *Governance:* W3C membership is open to companies, universities, governmental organizations, non-profit entities, and individuals.[16] However, the majority of the active members work for companies whose products employ web standards.[17] W3C is funded by its membership, based on a sliding scale adjusted for factors such as the location in the world and the type of entity.[18] Standards are adopted based on consensus through technical discussion and compromise among relevant members.[19] When there is a deadlock and all available means of consensus have been exhausted, a formal vote is conducted.[20]

iii. International Telecommunication Union's Telecommunication Standardization Sector ("ITU-T")

13. *What they do:* ITU-T is one of three sectors that comprise the International Telecommunications Union, a specialized UN agency dedicated to the development of

---

[11] Paul Hoffman (ed.), IETF, "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force," available at https://www.ietf.org/tao.html.

[12] RFC 2418 at 13; ARTICLE 19 submission at 12.

[13] While the Web has become synonymous with the Internet, it is one of a diverse range of applications that runs on and facilitates information exchange across the Internet. The Internet is the networking infrastructure that connects computers worldwide – in other words, the network of networks. Other Internet applications include e-mail, VoIP (Voice over Internet Protocol), mobile telephony, and peer-to-peer networks.

[14] See ARTICLE 19 submission at 12.

[15] See Free Software Foundation, "Keep DRM out of Web standards -- Reject the Encrypted Media Extensions (EME) proposal" (24 April 2013), *available at* https://static.fsf.org/dbd/Joint_Letter_on_W3C_HTML5_proposal.pdf. However, proponents claim that the specification will merely provide "a simple, easy to use way of putting encrypted content online." Tim Berners-Lee, "On EME in HTML 5" (28 February 2017), *available at* https://www.w3.org/blog/2017/02/on-eme-in-html5/.

[16] See World Wide Web Consortium, "Membership FAQ," *available at* https://www.w3.org/Consortium/membership-faq#who (stating "all types of organizations [including commercial, educational and governmental entities] and individuals").

[17] See W3C, Current Members," *available at* https://www.w3.org/Consortium/Member/List; see also DeNardis at 75.

[18] See W3C, "Membership Fees," *available at* https://www.w3.org/Consortium/fees (stating "W3C fees vary depending on the annual revenues, type, and location of headquarters of an organization").

[19] See W3C, "World Wide Web Consortium Process Document," § 3.3, *available at* https://www.w3.org/2017/Process-20170301/#Consensus.

[20] *Id.* at § 3.4.

Information and Communications Technologies.[21] ITU-T develops standards that "define how telecommunications networks operate and interwork", from landline networks to cable set top box architecture and broadband DSL.[22]

14. *Governance:* While these standards are non-binding and adopted on the basis of consensus, many of them have been widely adopted among States and the private sector. ITU membership comprises 193 States and more than 700 representatives from the private sector, non-governmental organizations, and academic institutions. Only States have voting rights.[23] However, non-State members may seek to influence the organization's proceedings and recommended standards through participation in each sector's Study Groups (which generates draft recommendations for adoption) and Sector Conferences (which define each sector's agenda and desired outcome every four or five years).[24] As the Internet supplants traditional telecommunications networks and systems, ITU's role in Internet standardization and governance is hotly contested. For example, ITU-T has established Study Groups focused on standardization for cloud computing and Internet of Things infrastructure.[25] Given that the ITU is an intergovernmental organization, however, some argue that its expanding role threatens the multi-stakeholder model of Internet governance that is critical to maintaining a free and open Internet.[26] Furthermore, ITU has drawn criticism for operating "a very exclusive, top-down decision making process", and lacking "transparency, openness, and inclusiveness".[27]

iv. European Telecommunications Standards Institute ("ETSI")

15. *What they do:* Unlike IETF, W3C, and ITU-T, which develop standards that apply globally, ETSI is a regional body focused on establishing European protocols for "fixed, mobile, radio, converged, broadcast and Internet technologies."[28] Nevertheless, these

---

[21] The other sectors are Radiocommunications (ITU-R), which allocates global radio spectrum and satellite orbits, and Telecommunication Development (ITU-D), which promotes the development of telecommunications infrastructure and services.

[22] International Telecommunication Union, "ITU-T Recommendations," *available at* https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx.

[23] ITU, "ITU World Telecommunication Standardization Assembly 2016: Background Paper" *available at* https://www.internetsociety.org/doc/itu-world-telecommunication-standardization-assembly-2016-background-paper.

[24] The ability to influence proceedings varies according to membership status. Becoming a non-state member of the ITU requires payment of membership fees, with different fees charged to private-sector, academic members, and non-governmental organizations. The membership fee for NGOs begins at 31,800 CHF. ITU, "Membership Fees," *available at* http://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx. While there are other membership options available at slightly cheaper rates, these memberships do not afford the same rights as full sector members, and do not grant the right to influence final decision-making. ITU, "Can any company or organization become an ITU-T member?" *available at* http://www.itu.int/net/ITU T/info/answers.aspx?Fp=faqs.aspx&Qn=11&ewm=False; ITU, "Participation Rights," available at http://www.itu.int/en/ITU-T/membership/Pages/Rights.aspx.

[25] ITU, "ITU-T Recommendations," *available* at https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx; Telecommunication Standardization Sector of ITU, "Resolution 2- ITU Telecommunication Standardization Sector study group responsibility and mandates," *available at* https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.2-2016-PDF-E.pdf.

[26] See, e.g., Internet Democracy Project, "The ITU and global Internet governance," available at https://internetdemocracy.in/issues/global-internet-governance-architecture/the-itu-and-global-internet-governance/.

[27] ARTICLE 19 submission at 11.

[28] European Telecommunications Standards Institute, "About ETSI," *available at* http://www.etsi.org/about (last accessed February 28, 2017). ETSI also develops standards that "provide the technical detail necessary" to execute European Commission mandates and directives.

protocols often have global reach and impact. For example, before the advent of 3G and 4G networks, the GSM standard developed by ETSI was the de facto global standard for mobile communications.[29] ETSI also participates in the development of standards for next generation mobile networks as a member of the 3rd Generation Partnership Project.[30]

16. *Governance:* ETSI is registered as a non-profit organization composed of more than 800 members, including manufacturers, network operators, service and content providers, national administrators, universities and research bodies, user organizations, and consultancy companies and partnerships.[31] Membership is fee-based and open to "any company or organization, from any part of the world, with a legitimate interest in [ETSI's] work".[32] Proposals to create a new standard or to update an existing one may come from members, the European Commission, or the European Free Trade Association, and require the agreement of four members to proceed.[33] Depending on the type of standard involved, adoption may require the approval of a select committee of members, the entire membership, or the European National Standards Organizations.[34] Historically, ETSI has considered both international and national legal bases for human rights obligations when developing particular technical standards.[35]

v. Institute of Electrical and Electronics Engineers ("IEEE")

17. *What they do:* IEEE is the world's largest technical professional organization, composed of over 400,000 electrical engineers, computer scientists, and related professionals from more than 160 countries. The organization conducts standards development through its dedicated outfit, the IEEE Standards Association ("IEEE-SA"). IEEE standards span a wide range of fields, including aerospace, healthcare, transportation, nuclear power, and wired and wireless communications services.[36] IEEE has also been engaged in the development of standards for artificial intelligence and autonomous systems, and in April 2016, launched a global initiative to address the ethical dimensions of this work[37].

18. *Governance:* IEEE-SA members submit proposals for standards projects (known as "Project Authorization Requests"), which must gain the approval of a sponsor (usually the IEEE society responsible for the scope and content of a proposed standard) and the IEEE-

---

The European Telecommunications Standards Institute, "Different Types of ETSI Standards," *available at* http://www.etsi.org/standards/different-types-of-etsi-standards.

[29] ETSI, "Our standards," *available at* http://www.etsi.org/standards.

[30] See discussion *infra*.

[31] ETSI, "Who are our members," *available at* http://www.etsi.org/about/who-we-are.

[32] *Id.*; see also ETSI, "What Does Membership Cost?," *available at* http://www.etsi.org/membership/fees#Members.

[33] ETSI, "How does ETSI make standards?," *available at* http://www.etsi.org/standards/how-does-etsi-make-standards.

[34] *Id.*

[35] See, e.g., ETSI, "Security Techniques Advisory Group (STAG); A guide to the legislative and regulatory environment," §6.1, *available at* http://www.etsi.org/deliver/etsi_etr/300_399/330/01_60/etr_330e01p.pdf; see also ETSI, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)," §5.2, *available at* http://www.etsi.org/deliver/etsi_ts/187000_187099/187016/03.01.01_60/ts_187016v030101p.pdf.

[36] Institute of Electrical and Electronics Engineers – Standards Association, "Technology Standards & Resources," *available at* http://standards.ieee.org/findstds/index.html; see also DeNardis at 76. Note that some of the most widely known IEEE standards—including the Ethernet Local Area Network standards and the Wi-Fi family of standards— concern wired and wireless communications services.

[37] IEEE-SA, "IEEE Standards Association Introduces Global Initiative for Ethical Considerations in the Design of Autonomous Systems," *available at* http://standards.ieee.org/news/2016/ieee_autonomous_systems.html.

SA Standards Board to proceed.[38] Working groups are subsequently convened to develop and draft the relevant standard.[39] Once the sponsor has determined that "the draft of the full standard is stable," the standard is submitted for balloting.[40] The goal of balloting is to "gain the greatest consensus", and a standard will pass if at least 75 percent of all eligible ballots are returned and if 75 percent of these bear a yes" vote.[41]A 60-day public review process, which provides an opportunity for the general public to submit comments on the proposed standard, is initiated simultaneously with the balloting process.[42]After ballot approval, the standard is submitted to the IEEE-SA Standards Board for final approval.[43] While non-members are permitted to participate in certain standards projects, only members are eligible for leadership positions.[44] To participate in balloting, IEEE-SA membership or payment of a "per-ballot fee" is required.[45] Pricing for corporate membership is determined on the basis of annual revenues of the corporation, and each corporation is permitted only one vote on ballots.[46]

vi. The 3rd Generation Partnership Project ("3GPP")

19. *What they do:* 3GPP is a collaboration between seven telecommunications standards associations worldwide: The Association of Radio Industries and Businesses, Japan; the Alliance for Telecommunications Industry Solutions, USA; China Communications Standards Association; ETSI; Telecommunications Standards Development Society, India; Telecommunications Technology Association, Republic of Korea; and Telecommunication Technology Committee, Japan (known as "3GPP Organizational Partners").[47] 3GPP has developed standards for 3G and 4G networks, such as UMTS and LTE specifications respectively.[48] It is a key actor in the development of 5G standards – the next generation of mobile networks and wireless systems at the time of publication.[49]

20. *Governance:* The private sector has significant influence of the work of the 3GPP. Industry groups representing the interests of Telcos, ISPs, and related businesses may, at the invitation of an Organizational Partner, take part in 3GPP's activities as a Market Representation Partner. While the latter "does not have the capability and authority to define, publish and set [3GPP] standards", they may nevertheless "offer market advice to 3GPP and … bring into 3GPP a consensus view of market requirements" relating to

---

[38] IEEE-SA, "Develop Standards: Submitting A Project Request," *available at* https://standards.ieee.org/develop/par.html.

[39] IEEE-SA, "Develop Standards: What Is A Working Group?," *available at* https://standards.ieee.org/develop/wg.html.

[40] IEEE-SA, "Develop Standards: The Balloting Process," *available at* https://standards.ieee.org/develop/balloting.html.

[41] *Id.*

[42] IEEE-SA, "Develop Standards: The IEEE-SA Public Review Process," *available at* https://standards.ieee.org/develop/publicrev.html.

[43] IEEE-SA, "Develop Standards: How Is Final Approval Obtained?", *available at* https://standards.ieee.org/develop/finalapp.html.

[44] IEEE-SA, "IEEE-SA Membership," *available at* https://standards.ieee.org/membership/index.html. Non-members may participate in the individual standards development process, but not the entity standards development process. See IEEE-SA, "FAQs: The Entity Standards Development Process," *available at* https://standards.ieee.org/faqs/cnm.html.

[45] IEEE-SA, "Develop Standards: The Balloting Process," *available at* https://standards.ieee.org/develop/balloting.html.

[46] IEEE-SA, "IEEE-SA Membership," *available at* https://standards.ieee.org/membership/index.html; *Id.*

[47] 3rd Generation Partnership Project, "Partners," *available at* http://www.3gpp.org/about-3gpp/partners.

[48] 3GPP, "Specifications Home," *available at* http://www.3gpp.org/specifications/specifications.

[49] 3GPP, "About 3GPP," *available at* http://www.3gpp.org/about-3gpp.

relevant telecommunications services, features, and functionalities. Notably, it does not appear that 3GPP provides similar opportunities for civil society, human rights groups, academics and others to provide input on the human rights impact of their work.

B. Incorporating Human Rights Considerations into Standards Development

21. The Special Rapporteur has joined a growing body of technical, academic and civil society experts calling for in-depth study of the human rights impact of technical standards and how standards development should seek to enable the exercise of human rights. While the current discourse largely focuses on the IETF's protocol design process, the key questions and issues discussed cut across all forms of standards development.

22. A survey of the relevant literature reveals a variety of approaches concerning the role of human rights in standards development, but two are particularly salient.[50] Some argue that the protocol design process should "bak[e]" into the architecture those "key, universal values" reflected in the Universal Declaration of Human Rights.[51] These human rights standards are widely accepted among the international community, even if their interpretation and implementation vary across social, political, and cultural contexts. In particular, values that are most relevant to protocol design and have a "fundamental impact on individual autonomy", such as freedom of expression and privacy, are "protected in the constitutions of many countries" and have "widespread democratic assent".[52]

23. Others, however, insist that protocol design should ensure that architecture design is flexible enough to accommodate a range of outcomes, including those that may be inconsistent with human rights, so that "the tussle takes place within the design".[53] In this view, limited understanding of the precise content of human rights and their accompanying parameters is a critical barrier to instantiating human rights through standards development.[54] Furthermore, since SDOs have neither the expertise nor legitimacy to make

---

[50] There are at least three other proposed approaches in the field: 1) design that, while not explicitly referencing human rights, nevertheless treats the Internet backbone as a public good and seeks to guarantee its "overall integrity and functionality"; 2) design that proceeds on the basis that Internet access (and potentially other Internet-related capacities) is in and of itself a human right; and 3) a 'wait-and-see' approach that supports more human rights education in the technical community but cautions against any definitive claims concerning the design process pending further research. For a fuller summary of these approaches see Niels ten Oever & Corinne Cath, Human Rights Protocol Considerations Research Group, IRTF, "Research into Human Rights Protocol Considerations," draft-irtf-hrpc-research-13 (May 18, 2017) *available at* https://tools.ietf.org/html/draft-irtf-hrpc-research-13. Additionally, the Human Rights Protocol Considerations Research Group, led by ten Oever and Cath, also proposes its own approach to incorporating human rights into protocol design, which is discussed *infra*.

[51] Ian Brown, David D. Clark, & Dirk Trossen, "Should Specific Values Be Embedded in the Internet Architecture," (2010) *available at* http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf.

[52] *Id.*

[53] David. D. Clark, John Wroclawski, Karen R. Sollins, and Robert Braden, "Tussle in cyberspace - defining tomorrow's Internet", IEEE/ACM Transactions On Networking, Vol. 13, No. 3 (June 2005) at 466, *available at* http://dl.acm.org/citation.cfm?id=1074049.

[54] Corinne Cath & Luciano Floridi "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights" L. Sci Eng Ethics (2017) 23: 449, *available at* https://link.springer.com/article/10.1007/s11948-016-9793-y.

or interpret human rights standards, such activity may trigger governments to abandon the current standards process, "effectively cleaving the Internet at the logical layer".[55]

i. The human rights impact of technical standards

24. These concerns require SDOs to tread cautiously, and may counsel against "hard-coding human rights into protocols".[56] However, they do not diminish the close connection between standards development and the exercise of human rights online. Like any technological development, standards do not simply serve technical functions. Instead, they are shaped by their historical and cultural contexts, reflect the assumptions and values of their respective developers, and influence public policy.[57]

25. Wittingly or not, the protocol design process already incorporates human rights values to varying degrees. For example, standards development focused on Internet accessibility for minorities and other vulnerable groups – such as the W3C's Web Accessibility Initiative to enhance web access for those with cognitive and physical disabilities – enhances their capacity to exercise freedom of expression online.[58] Edward Snowden's revelations about mass government surveillance have also prompted deeper scrutiny of the privacy implications of protocol design choices. In 2013, the Internet Architecture Board adopted guidance to "make designers, implementers, and users of Internet protocols aware of privacy-related design choices.[59] While the guidance approaches privacy breaches as "technical attack[s] that undermin[e] trust in the network", it nevertheless facilitates the exercise of the right to privacy and related human rights.[60]

26. Conversely, inadequate consideration of human rights has contributed to technical loopholes that render users vulnerable to access restrictions, privacy violations, and other human rights abuses. For example, the visibility of source and destination IP addresses in the IPvV4 protocol – a widely used protocol for data communication across different networks – has enabled censors to identify websites and network traffic for blocking or discrimination.[61] The lack of mandated Transport Layer Security (TLS) under HTTP connections has not only exposed users to third party interception of their communications, but also deliberate attempts to compromise the security of their devices.[62]

ii. Standards development and human rights considerations

27. While it is not always possible to encode human rights values during the protocol design process, developers and other stakeholders should nevertheless be sensitive to the human rights implications of their work. The perceived lack of expertise and legitimacy is not insurmountable. The business and human rights movement, which has navigated similar challenges, demonstrates that non-State are capable of adopting an incremental and credible approach to human rights accountability. In particular, SDOs may seek guidance from ICT companies that have adopted due diligence and responsibility-by-design measures as part of

---

[55] Jonah Force Hill, "A balkanized Internet? The uncertain future of global Internet standards," Georgetown Journal of Int'l Affairs, November 2, 2014, *available at* http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12707_Hill-CYBER-2012.pdf.

[56] draft-irtf-hrpc-research-13 at 11.

[57] See, e.g., Sandra Braman, "Internet Designers as Policy-Makers," (February 21, 2017) *available at* https://cyber.harvard.edu/events/luncheons/2017.02/Braman.

[58] DeNardis at 77-82.

[59] A. Cooper, H. Tschofenig, B. Abob, J. Peterson, J. Morris, M. Hansen, R. Smith Janet, Internet Architecture Board (IAB), RFC 6973 (July 2013), *available at* https://tools.ietf.org/html/rfc6973; Internet Society submission at 4.

[60] Cath & Floridi at 458; Internet Society submission at 6.

[61] draft-irtf-hrpc-research-13 at 21-22.

[62] draft-irtf-hrpc-research-13 at 26-27.

their implementation of the United Nations Guiding Principles for Business and Human Rights.

28 In this vein, the Human Rights Protocol Considerations Research Group of the Internet Research Task Force – an IETF affiliate that focuses on longer-term research issues – is developing guidance to facilitate "conscious and explicit design decisions" that take into account human rights considerations.[63] In particular, this guidance poses a series of questions on issues ranging from privacy to content agnosticism and internationalization that developers can take into account at "any point in the design process".[64] This methodology is similar to Human Rights Impact Assessments that several Internet and telecommunications companies conduct during the design and engineering phase of product development.

29. Policies and practices that facilitate a more transparent and inclusive protocol design process should also be encouraged. Meaningful access to information concerning "the development of a standard and associated deliberations, minutes, and records" provides opportunities for public input, establishing public accountability and oversight.[65] Increasing the participation of engineers with human rights expertise and civil society representatives will also empower SDOs to better identify and address the human rights impact of their work.[66]

III. Overview of Submissions Received in Preparation of A/HRC/35/22

30. The Special Rapporteur's call for input generated 25 submissions from States; 3 from companies; 22 from civil society, academics and others; and 1 confidential submission. The Special Rapporteur is extremely grateful for the submissions received, each of which informed, in one way or another, the report itself. The submissions referenced in this report may be found at the website of the mandate.

A. The Provision of Internet and Telecommunications Access: Freedom of Expression Issues and Concerns

i. Internet and Telecommunications Shutdowns

31. Various submissions discussed the scale, duration, and frequency of shutdowns, as well as the types of services affected. See Bahrain Center for Human Rights at 13, Access Now ("Access") Part I at 12, and Internet Sans Frontieres ("ISF") at 1. Access's submission also provides an overview of various domestic legal frameworks concerning the authority to order shutdowns. See Access Analysis of Shutdown Laws.

32. One submission discussed the technical means used to shut down networks or otherwise censor the Internet. In particular, network disconnection or adversarial route announcement, which "withdraws all of the Boarder (sic) Gateway Protocol (BGP) prefixes routing through the censor's country", is "perhaps the crudest of all censorship techniques" and has the effect of "shutting off the network". See Center for Democracy and Technology ("CDT") Part III at 16.

---

[63] Human Rights Protocol Considerations Research Group, https://irtf.org/hrpc.

[64] Content agnosticism is defined as the treatment of "network traffic identically regardless of content." draft-irtf-hrpc-research-13 at 43. Internationalization is defined as the "practice of making protocols, standards, and implementations usable in different languages and scripts." *Id.* At 44.

[65] DeNardis at 84.

[66] Cath & Floridi at 465.

33. Submissions highlighted common government justifications for shutdowns, and their incompatibility with international law. See ISF at 2, and Access Part I at 5.

34. Submissions also discussed the impacts of shutdowns, including their impact on the exercise of human rights other than freedom of expression, democratic and political participation, and the economy. See Access Part I at 2, Global Network Initiative ("GNI") at 4, and Telecommunications Industry Dialogue ("TID") at 2.

35. One submission proposed restricting the authority to conduct shutdowns through an amendment to the Constitution of the International Telecommunications Union. See Association for Proper Internet Governance.

36. Various submissions addressed the need for multi-stakeholder collaboration to address shutdowns. See GNI, Access Part I at 15-16.

ii. Other Forms of Content Blocking and Regulation

37. Although the report focuses on shutdowns, submissions discussed a wide variety of forms of online censorship.

38. Certain forms of censorship are directly conducted by States, which often grant government agencies broad authority to block or restrict access to a wide range of online content. See ARTICLE 19 submission at 2. For example, the National Authority for Management and Regulation in Communications of Romania ("ANCOM") has the authority to require ISPs to block certain "pornographic content, illegal gambling, or products likely to have psychoactive effects". See Romania at 1. Estonia's Gambling Act requires ISPs to "block access to online casinos which do not pay gambling taxes to Estonia". See Estonia at 1. In China, the government "deploys sophisticated technology, including the "Great Firewall", to monitor online communications, conduct surveillance, and block undesirable content". See Human Rights in China ("HRIC") at 1. China also "enlists voluntary company initiatives and the online community in monitoring and censoring expression". *Id.* at 28-30.

39. Other forms of censorship are conducted by private actors at the direction of States. Content blocking obligations are frequently "included directly in licensing obligations", requiring Telcos and ISPs to "block or filter certain types of content, such as pornography or otherwise contrary to "good morals". See ARTICLE 19 at 3. Telcos "can block access to entire websites, specific pages or specific keywords"; such blocking "prevents users from receiving information but can also prevent users from posting information to a specific location such as in the case of social networks". See Ranking Digital Rights ("RDR") at 9.

40. Several States mandate that ISPs must offer filtering services to their customers. Under Section 41 of Israel's Communications Law (Bezeq and Broadcasting) 5742-1982, ISPs are obliged to "notify subscribers regarding offensive websites and offensive content [as defined in the law], and the possibilities of protection against them, including technological means which are intended to filter such websites or content". See Israel at 2-3.

41. Copyright enforcement is another area of content regulation that raises significant concerns for freedom of expression. One submission notes that "copyright owners are increasingly seeking to enlist the assistance of [ISPs] to enforce copyright and impose sanctions on their users". See Nicolas Suzor ("Suzor") at 3. In Europe, the European Commission is reportedly "putting pressure on companies to "voluntarily" impose sanctions on online services accused of infringements". See European Digital Rights ("EDRi") at 3-4. For criticisms of Australia's copyright regime, see Digital Rights Watch ("DRW") at Section 2.

42. Various submissions discussed the human rights impact of content regulation on social media and other Internet platforms. See ADF International; Suzor. While these issues

are beyond the scope of the present report, the Special Rapporteur plans to address them in future reporting.

43. For an analysis of common network censorship techniques, including HTTP Request Header Identification, Deep Packet Inspection ("DPI") Identification, and TCP/IP Header Identification, see CDT Part III.

44. The Special Rapporteur has previously outlined the range of content regulation issues that implicate both States and the private sector (A/HRC/32/38 at para.10-12).

iii. Net Neutrality

45. Submissions discussed various forms of interference with net neutrality, and their impact on freedom of expression. For an overview of the "wide array of [network] traffic management practices [employed by Telcos and ISPs] resulting in undue restrictions", see Luca Belli ("Belli") at 3-4.

46. The benefits of zero rating and the risks they pose to freedom of expression are the subject of much debate, and depend to some extent on the type of zero rating arrangements at issue. Arrangements that offer unmetered access to certain applications, content or services without the purchase of a data plan (such as "Free Basics") are particularly contentious. Supporters argue that these arrangements facilitate freedom of expression by providing some degree of Internet access to areas that would otherwise lack connectivity. As more users go online with the assistance of these arrangements, the theory goes, the price of connectivity will be lowered, broadband infrastructure will improve, and digital innovation will increase. See CDT Part I (A) at 11. But these outcomes are far from guaranteed, and highly dependent on factors such as user behavior, market conditions and the regulatory environment. Users conditioned to rely on zero rated platforms might be reluctant to seek out new content and services. Well-established platforms might also be able to secure better terms of access to zero rating arrangements than smaller competitors, reinforcing their dominance and their impact on user choice. Finally, the continued presence of zero rating in an emerging market could incentivize low data caps and inflate the price of metered data, even as Internet adoption increases. At the very least, whether and how zero rating might lead to Internet adoption while minimizing the risk of creating permanently walled online gardens is in need for further study. See CDT Part I (A) at 15. See also Access Part II at 18-19; Fundacion Karisma at 6-7.

47. Various States discussed domestic efforts to regulate and protect net neutrality in their submissions. Estonia and Slovakia stated that they had implemented relevant European Union net neutrality regulations in their domestic law. Bulgaria stated that net neutrality regulation should be "directed towards finding a balance between preserving the open character of the Internet and guaranteeing the fundamental rights of consumer", and that on certain aspects of net neutrality (such as quality of service issues and anti-competitive blocking), "there should be an opportunity for intervention of a competent authority". See Bulgaria at 5. Norway stated that its guidelines on net neutrality seek to ensure that the Internet remains "an open and non-discriminatory platform for all types of communication and content distribution". See Norway at 5. EDRi's submission also highlighted the Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, adopted by the Body of European Regulators ("BEREC").

48. Telefonica was the only company that provided input on the issue of net neutrality. Telefonica's position is that it understands the need for the "protection of users' rights and their freedom of user choice", but at the same time claims "the ability to manage traffic on our networks, and permit differentiation of Internet access service". See Telefonica at 1-2.

49. One submission highlighted the Model Framework on Network Neutrality developed by the Dynamic Coalition on Network Neutrality, a multi-stakeholder initiative of the UN Internet Governance Forum. See Belli.

iv. Government Access to User Data

50. Concerns regarding government access to user data held by the private sector were a persistent theme throughout the submissions. See, e.g., EDRi (discussing provision or facilitation of access to consumer data in the EU); CDT Part I (B) (outlining a descriptive framework and a normative framework for analysing and comparing domestic laws on surveillance and government access to user data); RDR (analyzing telecommunications companies' disclosures to users about how their information is handled); DRW (discussing remedies for undue access to customer data).

51. Various submissions raised human rights concerns arising from direct access to Internet and telecommunications networks – a practice that is still shrouded in secrecy. See Privacy International ("PI"); TID at 3; CDT Part I (B) at 30; Fundacion Karisma at 1 (discussing Colombia's law requiring installation of networks that enable government access).

52. Many submissions discussed data retention requirements imposed by governments on private actors, and the privacy concerns these create. See submissions of CDT Part I (B) at 31; Access Part II (analysing data retention in Latin America and the EU); Fundacion Karisma at 2 (discussing Colombia's data retention and mobile registration requirements); Bahrain Center for Human Rights at 17 (discussing Bahrain's data retention requirements); DRW at Section I (discussing Australia's data retention regime); HRIC at 12 (discussing data localization and real name identification laws in China).

53. States' submissions illustrate the range of legislative and regulatory frameworks that authorize government access to customer data. States that provided information concerning relevant laws and regulations include: Bulgaria (Article 304 of the Electronic Communications Act); Canada (Section 37 of the Telecommunications Act); Estonia (Section 111 and 113 of the Electronic Communications Act); Finland (Section 185 of the Information Society Code); Georgia (Article 8(1) of the Law of Georgia on Electronic Communications); Japan (Telecommunication Business Act); the Philippines (Anti-Wiretapping Law, Cybercrime Prevention Act)); Serbia (Section 17 of the Law on Electronic Communications); and Slovakia (Part 4 of the Electronic Communications Act, titled Protection of Privacy and Personal Data). Notably, Canada and Japan require judicial pre-authorization for certain forms of government access.

54. Submissions also raised concerns about the lack of government transparency concerning their access to user data. See, for example, CDT Part I (B) at 15 (discussing vague and ambiguous laws, opaque surveillance practices, inadequate oversight and reporting mechanisms, and the lack of transparency concerning voluntary data sharing); Access Part II at 15-16 (discussing government non-compliance with transparency obligations under their own domestic laws); PI (discussing general lack of transparency concerning direct access); and GNI at 3-4 (observing that "many governments' legal frameworks continue to prohibit publication of [information about government requests for user data] by companies").

55. On the other hand, a few governments have established transparency measures that appear to be a step in the right direction. For example, Canada adopted "Non-binding Transparency Reporting Guidelines" that aim to help "private organisations [be] open with their customers regarding the management and sharing of their personal information with government entities such as law enforcement and national security agencies". See Canada at 8. In Finland, under the Act on the Openness of Government Activities (621/1999), "all official documents are in the public domain, unless their publication has been specifically restricted". See Finland at 6.

56. Human Rights concerns associated with government access to user data have been addressed in the Special Rapporteur's previous reports. In particular, the Special Rapporteur has previously analyzed threats to encryption and anonymity (A/HRC/29/32),

and the human rights impact of communications surveillance (A/HRC/23/40). The UN Office of the High Commissioner for Human Rights has also analyzed the protection and promotion of the right to privacy in the context of domestic and extraterritorial communications surveillance (A/HRC/27/37).

v. Digital Inclusion and Accessibility Concerns

57. A few submissions also addressed the continued lack of Internet access in many parts of the world. In Latin America, for example, one submission observed the need to "complement infrastructure-deployment initiatives and regulatory reforms with targeted programs aimed at addressing connectivity barriers", such as "incentives for the creation of online content and services in indigenous languages", kindergarten to grade 12 school connectivity initiatives, and residential access subsidies for low-income families. See Global Commission on Internet Governance at 1. In Australia, one submission observed that the "significant digital divide" in the country has a particularly detrimental impact on "older Australians, indigenous people and people with disabilities, among others". See IIRW at Section 6. It also argued that "competition and consumer laws are … important to closing the digital divide". *Id.*

II. The Human Rights Responsibilities of the Digital Access Sector

i. Developments in Multi-Stakeholder Governance

58. On 27 March 2017, the Global Network Initiative ("GNI") expanded its membership to include six Telcos/ISPs and one network equipment vendor. The seven new members were formerly members of the Telecommunications Industry Dialogue ("TID"). When they joined the GNI, the TID ceased to be a functioning entity. The full list of GNI members may be found on its website.

59. Since the publication of the Special Rapporteur's main report (A/HRC/35/22), the GNI has also updated its Principles on Freedom of Expression and Privacy ("Updated GNI Principles"), as well as the accompanying Implementation Guidelines ("Updated GNI Guidelines"). These documents may be found on its website. Although there is significant overlap between the updated versions and the versions relied on in the main report, there are notable differences, some of which are noted below.

ii. Due Diligence

60. TID's submission discusses how member companies conduct Human Rights Impact Assessments ("HRIA") and other due diligence measures. TID at 7-8. GNI's submission discusses its Independent Company Assessment process, a "review of relevant internal systems, policies and procedures for implementing the GNI principles". See GNI at 8.

61. In separate submissions, Telefónica and Yahoo! explain their respective HRIA and due diligence processes in greater detail.

62. The Updated GNI Guidelines appear to contemplate a range of due diligence processes and mechanisms other than HRIAs. See Guidelines 2.4-2.7. Examples of business activities that should trigger due diligence are also identified. See Guideline 2.6.

63. The submissions identified several examples of HRIAs and due diligence measures.

64. In 2012, Telefónica, with the support of Business for Social Responsibility ("BSR"), conducted an HRIA "of all our operations to assess the global impact of our activitiy". Telefónica is continuing to integrate the results of the HRIA across its business operations. In 2015, Telefónica implemented "[p]eriodical reviews of the most significant risks in matters of privacy and security which affect our business at a global level". See Telefonica at 5.

65. In 2014, Orange "worked with Maplecroft to implement a customized risk index encompassing the 30 countries in which it is present as a mass-market operator". See TID at 7.

66. From 2015 to 2016, Telia Company, with BSR's support, conducted an HRIA of its plans to divest its Region Eurasia businesses. See TID at 7.

67. Nokia uses a "human rights due diligence process" to "identify potential risks for product misuse and to investigate ways to mitigate these risks". Flagging of potential risk cases is "embedded in the company's sales tool as an automated feature, thus minimizing the risk of missing any cases due to human error". See TID at 7.

68. Yahoo conducts "short-form" HRIAs for "specific, targeted questions" and "long-form" HRIAs when it "identifies significant risks to users' free expression and/or privacy". See Yahoo at 6-7.

69. HRIAs may lead to significant changes in a company's business plans and product or service design. For example, Yahoo's HRIA on its entry into Vietnam led the company to "manage and operate out Vietnamese language services out of Singapore so the services would be governed by laws with stronger protections than those in Vietnam". See Yahoo at 7.

iii. Stakeholder Engagement

70. Various submissions discussed ongoing and potential efforts to address threats to freedom of expression through collective action and multi-stakeholder collaboration. See, for example, PI (urging collective action to "bring transparency to [direct access] and begin to raise standards within a country and set best practice"); TID at 0-1 (discussing TID's efforts to "make available guidance and information on the main laws, regulations and standards that are applicable to licensed operators"); and GNI (discussing collaboration to address network shutdowns).

iv. Mitigation Strategies

71. The submissions identified examples of company policies and practices developed to handle government requests for content restriction and user data.

72. AT&T trains relevant employees to "confirm that requests are duly issued by an appropriate entity, under valid legal authority and ... otherwise in compliance with applicable requirements". The review process may include AT&T lawyers and where necessary, local counsel familiar with applicable law. See TID at 8.

73. Millicom finalized its "Guideline for Law Enforcement Assistance Requests" in 2015, which establishes procedures for handling, among other things, "urgent and non-written requests, how to log requests and our responses, how to protect customer data through the process of retrieving information, and how to deliver the information safely". See TID at 8-9.

74. The submissions also identified company strategies to mitigate or minimize the potential human rights impact or unlawful government demands or action.

75. In the past, Millicom and Orange have insisted on written government requests that comply with all necessary formatting and procedural requirements. See TID at 9.

76. Orange is also "setting up an emergency procedure" that sends an alert to the GNI, NGOs and other relevant stakeholders when it receives an unlawful or otherwise "unacceptable" government request. See Orange at 1.

77. Telenor "engages actively with relevant authorities", seeks clarifications on problematic requests, and, when needed, engages "diplomatic channels and international

organizations". Telenor also raises the need to "engage in longer-term dialogue, and not only when an incident occurs". See TID at 10.

78. When dealing with government requests, both TID and GNI emphasize the need to "[a]lways seek to ensure the safety and liberty of company personnel who may be placed at risk". See TID at 10-11; Updated GNI Principles, Principle 4 on Responsible Company Decision making.

v. Transparency

79. Various submissions highlighted areas where greater corporate transparency should be encouraged.

80. RDR, a "project to benchmark the world's largest internet, telecommunications, and other ICT companies" on their policies and practices affecting freedom of expression and privacy, identified several areas where greater corporate transparency is required. On network shutdowns, RDR found that less than half of the Telcos and ISPs it examined disclosed whether they notified users of access restrictions, and even fewer provided information about their process for responding to shut down requests. See RDR at 7- 8. RDR also urged companies to provide meaningful information concerning the "blocking and filtering practices of internet access services" they operate, as well as their network traffic management practices. See RDR at 9 - 10. Additionally, RDR found "industry-wide incoherence in disclosures to users about how companies handle their information," including "what is collected, how it is collect, how long it is retained, and with whom it is shared". See RDR at 11 - 12.

81. PI's submission contains specific recommendations on how companies can collectively seek to bring transparency to the "highly secretive process" of direct access.

82. GNI observed "despite increasing numbers of Telcos and ISPs adopting the practice of releasing transparency reports with information about government requests for user data, many governments' legal frameworks continue to prohibit publication of such data by companies". See GNI at 3.

83. Several Telcos and ISPs provided information on their transparency policies and practices. For example, Telenor stated that transparency "is not always easy, and in some instances, may have unintended and negative effects on efforts to minimize the impact on privacy and freedom of expression"; nevertheless, its stance "is to be transparent and this is communicated to the relevant authorities". See TID at 10. Telia Company has "made publicly available its internal tool for assessments and escalation of government requests and demands with potentially serious impacts on freedom of expression in communications", and has also begun to "report publicly on unconventional requests and demands with potentially serious impacts on the right to freedom of expression". See TID at 12, 14.

vi. Effective Remedies

84. Under the Updated GNI Guidelines, member companies are required to develop grievance mechanisms for users to raise "grievances about issues related to freedom of expression and privacy to be communicated to the company for consideration". Additionally, if a member company "determines its business practices are inconsistent with the [Updated GNI] Principles or have caused or contributed to adverse impacts, it will establish by itself or in cooperation with other actors, a means of remediation, including meaningful steps to prevent recurrence of such inconsistency or impact". See Guideline 2.13 (f).

85. RDR evaluates the effectiveness of a company's grievance and remedy mechanisms based on whether the company: (i) discloses its processes for receiving complaints or grievances, (ii) lists the kinds of complaints it is prepared to respond to, (iii) articulates its

process for responding to complaints, (iv) reports on the number of complaints received, and (v) provides evidence that it is responding to complaints, including examples of outcomes. See RDR at 6.

86. Access Now has developed a Telco Remedy Plan that provides guidance on the implementation of "the procedural aspects of remedy, such as safe and accessible grievance mechanisms, and the substantive aspects, which may be as simple as an explanation and commitment to non-repetition". Access Part II at 23.

87. The State potentially plays a critical role in ensuring access to effective remedies for violations of freedom of expression and privacy. In Australia, the Privacy Principles establish "a complaint process for individuals who believe they have had their privacy breached". Complaints are assessed by the Information Commissioner, and may result in civil penalties. See DRW at Section 5. Bharti Airtel, a Telco in India, scored the highest on RDR's survey of corporate grievance and remedy mechanisms, "due primarily to India's regulatory requirements in relation to remedy". See RDR at 6.

vii. Other Private Actors

88. One submission noted that, in the context of direct access, "there are other companies in the ICT ecosystem where [their] role … [is] less clear" and "needs to be explored". In particular, network equipment vendors, Internet Exchange Points, and submarine cable providers are among the companies that require further scrutiny. The role of Internet companies in establishing and managing undersea cables is also relevant. See PI at 8-9.

IV. Summary of Multi-Stakeholder Consultation on Human Rights Due Diligence and the Digital Access Industry

89. The Special Rapporteur co-organized and participated in four meetings that helped inform the main report: (1) an informal brainstorming session hosted by ARTICLE 19 in London on 22 July 2016; (2) an experts meeting hosted by the University of Connecticut on 24 October 2016; (3) a regional consultation with the Special Rapporteur on Freedom of Expression for the Inter-American Commission on Human Rights, hosted during the Internet Governance Forum in Guadalajara on 5 December 2016; and (4) a regional meeting in Beirut, hosted by the Special Rapporteur on 29 February - 1 March 2017, that touched in part on the issues in the report. The Special Rapporteur also conducted a special preview of the report hosted during RightsCon in Brussels on 30 March 2017.

90. This section summarizes the 24 October 2016 consultation hosted by the University of Connecticut. This consultation focused specifically on understanding the nature and scope of a company's obligation to engage in due diligence to assess human rights impacts in the Internet and telecommunications access industry. The private actors at issue included Telecommunications Providers ("Telcos"), Internet Service Providers ("ISPs"), Network Equipment Vendors ("Vendors"), Internet Exchange Points ("IXPs"), and Submarine Cable Providers.

91. The consultation was organized around four themes: Identifying Human Rights Risks, Due Diligence Practices and Procedures, Remedies, and Transparency. The discussion was held under modified Chatham House Rules: While participants are listed below, comments are not attributed to particular speakers or participants, nor are the opinions and interventions noted in this summary intended to suggest shared agreement on those points among the participants.

92. Seventeen participants (excluding the Special Rapporteur and his team) attended the consultation (affiliations listed here for identification purposes only): Barbora Bukovská (ARTICLE 19), Camilla Goldbeck-Löwe (Ericsson), Leslie Harris (Harris Strategy Group),

Patrik Hiselius (Telia Company), Rikke Frank Jørgensen (Danish Institute for Human Rights), Nicole Karlebach (Yahoo), Molly Land (University of Connecticut), Rebecca MacKinnon (Ranking Digital Rights), Peter Micek (Access Now), Charles Mok (Hong Kong Legislative Council), Laura Okkonen (Nokia), Moira Oliver (British Telecom); Milka Pietikainen (Millicom), Lucy Purdon (Privacy International), Michael Samway (Georgetown University), David Sullivan (Global Network Initiative), Niels ten Oever (ARTICLE 19), Alexandria Walden (Google), Richard Wilson (University of Connecticut), and Cynthia Wong (Human Rights Watch).

93. The consultation was made possible by the financial support of the University of Connecticut's Humanities Institute, School of Law, and Human Rights Institute.

94. The report reflects points raised during the consultation but does not necessarily reflect the views of the Special Rapporteur or all participants.

A. Session 1: Identifying Human Rights Risks

95. In this session, participants discussed the variety of risks to human rights that Telcos, ISPs, vendors, and others may encounter in their daily operations, both in terms of compliance with local law as well as risks associated with the development of products, services and business strategies.

i. Engaging more actors

96. There was a general consensus among participants that the discussion about human rights risks should include actors beyond Telcos and ISPs, such as vendors, IXPs, and submarine cable providers.

97. Participants noted, hwoever, that it was less clear how to evaluate the human rights responsibilities of vendors, and that an understanding of how they operate and network equipment technology would be essential. It was agreed that these companies present unique challenges and there was a need for a more concrete understanding of the human rights risks their businesses face or create, ongoing efforts to address them, and accountability gaps.

98. Participants suggested that submarine cable providers should be more transparent regarding their contracts and their arrangements with governments. They noted several issues of specific concern, including: (i) Do Telcos / ISPs require minimal standards on the integrity/authenticity of the interface with submarine cable providers? (ii) What is the nature of the submarine cable provider's responsibility to secure the cables? (iii) Are there human rights issues associated with the cutting of cables? (iv) What are the terms of the contractual relationships and which actors are involved?

ii. Imprecise or vague legal standards

99. Participants emphasized the risks associated with imprecise or vague legal standards governing censorship and surveillance.

100. Concern was raised, for example, about the vague and open-ended nature of cybercrime laws that ban "disturbing", "annoying", or "inciting" online content, which are employed to censor and chill expression online. Reform of these laws should take into account how they are being enforced. How companies interpret and implement these laws is also critical.

101. One participant recommended that companies should work with the Global Network Initative ("GNI") to lobby for meaningful limits on content regulation and surveillance laws.

iii. Requests for website blocking and access to users' data

102. Participants noted that governments frequently demand that Telcos and ISPs block websites and hand over communications content and metadata, often without a valid judicial order.

103. Participants suggested that governments should be more transparent about their content takedown and surveillance requests, and should provide transparency reports on the volume and scope of such requests, and the number of such requests made with a warrant.

104. Participants mentioned that some ISPs integrate procedural safeguards into their licensing contracts, specifying, for example, the procedural steps to be followed when a government requests website blocking or access to user data. It was suggested that more companies should do this and perhaps go even further in specifying that requests must be in writing, signed by a responsible individual, identify the legal basis for the request and the time period for implementations, and set out the process for challenging the request.

105. Participants suggested that companies track the number of requests received for website blocking or access to user data, the identity of the requesting entity, the nature of the request, and the form of the request. They mentioned that such practice will make it easier to identify relevant, observable trends over time and will also allow the company to communicate to stakeholders transparently about its efforts to addres its human rights impacts.

106. Participants also expressed concern that customers and users are not aware of their rights. When local Telcos and ISPs do not themselves value transparency, participants noted that consumers are likely unaware of their rights and of the company's record. They suggested that advocacy groups should do more in term of public education efforts.

B. Session 2: Due Diligence Practices and Procedures

107. In this session, participants discussed the practices and procedures that Telcos, ISPs, and vendors might employ to assess and address their human rights risks and impacts.

i. Standardization

108. Some participants expressed the need to have a clear set of standards with regard to due diligence. The lack of agreed upon standards makes it harder for companies to report data that can be compared across the industry.

109. Some argued in favor of concrete guidance for how companies engaged in Internet and telecommunications access should implement the United Nations Guiding Principles on Business and Human Rights ("UN Guiding Principles").

110. Others argued that it would not be possible to have a standardized due diligence process across the industry or even a particular category of actors (e.g. among Telcos), since each company may have different needs, responsibilities, organizational structures, and internal processes.

111. Participants noted that, at a minimum, companies should disclose their policies and practices to ensure respect for human rights.

ii. What is Due Diligence?

112. Participants first considered the definition of due diligence, the scope of activities covered, and the relationship between due diligence and Human Rights Impact Assessments ("HRIA").

113. Many participants agreed that a company should publicy announce its commitments to the UN Guiding Principles. However, this alone is not sufficient. Companies must also

follow up on their commitments by translating these principles into due diligence policies and practices that are triggered during relevant business activities, such as the design and engineering phase of a new product, product modification, or market entry. Companies should ensure that due diligence is conducted not only by employees but also relevant corporate partners and agents.

114. Several participants agreed that robust due diligence include at least the following steps: (i) analysis of governing human rights laws and standards, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the UN Guiding Principles, and the GNI Principles; (ii) understanding the human rights landscape of the relevant market with particular focus on rule of law, freedom of expression and privacy; (iii) considering the impact of relevant local laws on freedom of expression and privacy; (iv) connecting business plans to potential human rights risks and opportunities; (v) considering how the product could promote human rights, for example by enhancing access, education, communication, or privacy; (vi) evaluating the risks based on the company's products and operations, including the severity and likelihood of the risks, in consultation with stakeholders; and (vii) developing a strategy for mitigating risks and protecting human rights.

iii. Human Rights Impact Assessments

115. Participants discussed HRIAs as a means of due diligence. HRIAs inform and guide evolving corporate strategies to ensure respect for their customers' right to freedom of expression and privacy.

116. Some noted that while HRIAs have been promoted as a due diligence tool, there should be a better shared understanding of what precisely these assessments require or entail.

117. Participants suggested companies may appear to be more credible if HRIAs are outsourced to an independent expert or body of experts.

iv. Why Due Diligence?

118. Participants discussed how due diligence can contribute to effective risk management.

119. Due diligence may integrate a more rights sensitive culture within the company, mainstreaming human rights considerations within corporate thinking and decision-making.

120. Companies might develop greater ownership of their human rights performance as they consider the human rights issues they face during the process of policy development and reflection on existing practice, rather than primarily engaging with human rights only when they are subject to external challenge.

v. When to Conduct Due Diligence?

121. Participants also discussed how often a company must engage in due diligence.

122. Participants emphasized that due diligence should be conducted regularly and on an ongoing basis, and not simply to address one-off events. Ongoing due diligence enables a company to understand how its risks can change over time and how to manage them effectively.

123. Participants identified the need for more clarity on the types of business activities that trigger due diligence, and greater corporate transparency concerning these triggers. Triggers could include changes in the political environment, new laws, contract renewals, change of service, or market entry.

124. Mergers and acquisitions are also a trigger point, although one participant pointed out that it might be difficult to conduct due diligence in the context of a contractual negotiation, since the only information provided is public information. Therefore, it might be more appropriate to conduct post-acquisition due diligence.

125. It is essential to address human rights issues at the earliest stages of business relationships to minimize situations where the company has little leverage to mitigate or avoid adverse human rights impacts.

126. Participants also noted the importance of due diligence in terms of the design of products and services.

vi. Who is Part of Due Diligence?

127. Participants discussed the types of employees and internal teams that should be engaged in due diligence processes – these include senior management, cross-functional human rights teams with senior oversight, investors, and external stakeholders.

128. A number of participants supported the involvement of senior management, which sets the tone throughout the company. At a minimum, the board of directors, corporate executive officers, and other senior excutives should actively support the company's commitments to human rights and understand their own roles and responsibilities in ensuring the company fulfils its commitments in this area.

129. Participants also agreed that due diligence should be conducted by cross-functional human rights teams with senior oversight, and include employees from the legal, policy, business functions, and engineering teams. Such teams send a signal that human rights concerns are the responsibility of the entire business enterprise. One participant noted that such teams should be led by employees with human rights expertise.

130. Engineers are particularly important because they have technical expertise concerning the company's products and services, and can significantly inform the design of technology-oriented approaches to mitigating or preventing adverse human rights impacts (such as design modification).

131. A specialized human rights team not only facilitates rapid responses to human rights crises, but also enhances the company's ability to pre-empt and avoid such crises.

132. A few participants noted that investors can play a very important role in incentivizing companies to recognize their human rights risks.

133. Participants also suggestd that external stakeholdesr should be involved in the due diligence process. Ongoing interaction and dialogue between a company and affected stakeholdesr, such as civil society representatives and other rights holders, enable the company to respond to their interests and concerns.

vii. Transparency

134. Several participants emphasized the need for greater corporate transparency concerning internal due diligence processes and practices – at a minimum, companies should disclose when they conduct due diligence, and high level summaries of the HRIA results.

viii. Outstanding Issues

135. Participants identified the following questions and issues that require further discussion: (i) How should a company with diversified services and multiple business models identify due diligence triggers and standardize due diligence processes across its operation? (ii) What are the costs (financial, time and otherwise) associated with due diligence? (iii) How much weight does / should a company assign to due diligence findings

and recommendations in their overall decision making process? (iv) What other trigger points exist beyond compliance with government requests? (v) When companies are already established in a market that poses human rights concerns, what can they do to mitigate or prevent adverse human rights impacts? How can they support rights-oriented legal and policy reforms?

C. Session 3: Remedies

136. In this session, participants discussed the types of remedies that should be available to Internet users when their human rights are violated.

i. The Government's Role

137. The role of the government in providing or facilitating access to an effective remedy was discussed.

138. In addition to the UN Guiding Principles, participants noted that European Court of Human Rights jurisprudence provides guidance on the content of the right to an effective remedy. According to the Court, an effective remedy requires recognition of the violation, the provision of satisfaction or compensation, and the establishment of sufficient grounds to avoid its recurrence.

139. Several participants noted that, under the UN Guiding Principles, the State bears the primary duty to ensure remedies; however, most States have not paid sufficient attention to this pillar of the UN Guiding Principles.

140. Others emphasized that the UN Guiding Principles also recognize a role for non-State remedies: Without a remedy provided by the State, rights holders often have to rely on the company.

141. Participants noted that Telcos and ISPs operate in a complex domestic and international legal system with various avenues for remedy. These include State-based judicial mechanisms, international organizations such as the OECD (Organization for Economic Co-operation and Development), national human rights institutions, and multi-stakeholder initiatives. One participant suggested that OECD's national contact points also provide a mechanism to bring human rights complaints against companies.

ii. Jurisdiction

142. Participants noted that the frequently cross-jurisdictional nature of human rights violations on the Internet complicates the ability of both State and non-State actors to provide an effective remedy.

143. Most countries' domestic legal frameworks give greater protection to the privacy rights of citizens than non-citizens, but the obligation of states to respect rights is not limited to the rights of persons physically in their territory.

144. Participants noted, however, that this view is contested and some governments have denied that their obligations extend to actions undertaken outside their territory. At the very least, however, territorial jurisdiction may arise on the basis of physical location or where the data is processed.

iii. Types of Remedies

145. The types of remedies that might be appropriate for human rights violations by Telcos, ISPs and associated companies was the subject of considerable discussion.

146. Participants noted that there are many different types of remedies including but not limited to recognition, satisfaction, non-repetition of violations, compensation, and

restitution. The remedy must be proportional to the harm. Participants also discussed the use of individual versus collective remedies.

147. Other participants noted that other kinds of remedies may be appropriate, such as disclosing information about the violations (such as HTTP 451, a landing page that explains why a webpage is unavailable), or commitments to non-repetition. In the ICT context, many victims are not seeking compensation; instead, they would rather be restored to the place they were before the violation.

148. Participants observed the importance of transparency concerning the violation in order to enable access to an effective remedy. Privacy concerns, however, may limit transparency. Furthermore, since many violations are triggered by local laws and other forms of State action, an appropriate remedy might require revealing the State's role – disclosures that many companies are unable or unwilling to make.

149. Remedies may be judicial or non-judicial, and non-judicial remedies may be integrated into a self-regultaory process. The GNI, for example, may provide a venue for the design and implementation of appropriate remedies.

iv. Grievance Mechanisms

150. Participants discussed the procedural elements of a grievance mechanism.

151. Participants suggested that companies should create grievance mechanisms to address users' complaints about potential human rights violations. Several GNI member companies have made commitments to establish grievance mechanisms.

152. One participant suggested that pre-existing complaints or whistleblowing hotlines provide a model for human rights grievance mechanisms. However, any channel of communication between the company and its users should be adequately secure and accessible.

153. Some ISPs have created a whistleblowing system to deal with corruption, and this could also be used to address human rights violations.

v. Other Issues and Challenges

154. Some participants noted that it could be difficult in some situations to identify the harms for which a company should be responsible. Under what circumstances is a company responsible? Under what circumstances should they provide a remedy? How closely related must the harm be to their activities?

155. Several discussed the distinction between human rights harms and non-human rights harms. Does the obligation to provide a remedy extend to both? How should these be distinguished? Participants noted, for example, that it is unclear whether a company should be responsible for economic harms arising from a government-ordered shutdown.

156. The large number of complaints that companies receive also poses logistical challenges. Additionally, a large number of complaints require translation, and raises issues of political, cultural and social context.

157. A few participants were also concerned that a narrow conception of remedies my disincentivize companies from making the structural changes needed to prevent or mitigate future violations.

158. Participants also asked about the role of the investor. A participant suggested that investors should be urged to create a socially responsible investment fund.

D. Session 4: Transparency

159. Participants discussed the need for companies to disclose information that meaningfully informs users about the human rights risks and harms associated with their products and services.

i. The Value of Corporate Transparency

160. Several participants discussed the importance of making a case to companies that transparency can be good for business. Transparency can be a boon to a company's brand. Healthy competition between companies about what they disclose and how effectively they disclose such information may meaningfully enhance transparency. Companies that face significant risks to their reputation in the event of non-disclosure are naturally inclined to innovate in this area.

161. Those pushing for heightened corporate transparency, however, must be sensitive to the need to protect trade secrets and the legal and regulatory environment in which these companies operate.

162. New companies require guidance on the need to create transparent due diligence processes and other transparency measures from the outset.

163. Current transparency practices concerning due diligence processes were also discussed. Some companies disclose information about HRIAs but others do not even disclose the fact that they conduct assessments. Companies should at least disclose when they perform HRIAs, and a summary of high-level findings.

164. Companies also play a critical role in pushing governments for more transparency.

ii. Challenges to Corporate Transparency

165. Participants discussed challenges concerning transparency reporting and standards.

166. Many participants agreed that minimum standards of disclosure should be established. However, these should not be so rigidly defined that they become a check-the-box process and deter transparency innovation.

167. Transparency reporting is insufficient. In addition to regular reporting, companies should also address the need to make disclosures in real time that respond to rapidly evolving situations (such as complicated product rollout or an evolving crisis).

168. Areas where corporate transparency can be improved include: information concerning the number of and reasons for website blocking and network shutdown incidents (including copyright takedowns and private defamation claims); the human rights implications of mergers and acquisitions; human rights risks associated with the use or misuse of products or services; and the nature and frequency of security updates, among others.

iii. Transparency Standards for Vendors and Submarine Cable Providers

169. The comparative lack of transparency measures for companies other than Telcos and ISPs was discussed.

170. Participants were concerned that non-consumer facing companies, such as vendors and submarine cable providers, have less incentive to adopt transparency measures. Submarine cable providers in particular have reportedly expressed skepticism concerning the relevance of human rights to their business. Companies that specialize in the design and sale of surveillance and monitoring equipment may have even less incentive to be transparent about their customers and practices.

171. Vendors are no longer simply selling routers and switches, but also network monitoring systems (e.g. Deep Packet Inspection) and associated training and consultation services. The human rights risks associated with these products and services require further study and analysis, and it is unclear whether and how vendors conduct human rights due diligence during their design and sale.

172. Forensic analysis of products currently on the market may reveal design flaws and security risks. Open-source design efforts may also mitigate human rights risks associated with "closed" systems.

173. For submarine cable providers, it might be helpful for civil society and the public to access cable leasing contracts, the parties that have access to a cable, and the circumstances under which cables may be cut or otherwise interfered with.

United Nations A/HRC/35/22/Add.5

General Assembly

Distr.: General
30 May 2017

English only

Human Rights Council
Thirty-fifth session
6-23 June 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Japan: comments by the State

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the comments by the State on the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Japan.

GE.17-08631(E)

Please recycle

Report of the Special Rapporteur the promotion and protection of the right to freedom of opinion and expression on his mission to Japan: comments by the State*

Response to recommendations

The draft report of Mr. David Kaye, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on the situation of freedom of expression in Japan which is to be submitted to the Human Rights Council was shared with the Government of Japan. The Government of Japan understands that in his draft report the Special Rapporteur delivers his own opinion on the recent situation of freedom of expression in Japan, in relation to areas such as Article 4 of the Broadcast Act, the Specially Designated Secrets Act, and hate speech.

However, as for the facts pointed out in the draft report, most of them are based on hearsay information or assumptions and do not show any verification of the details of related information. Based on these facts, the recommendations written in the draft report regrettably contain inaccurate and insufficient statements on the actual situation in Japan and Japanese culture, as well as arguments not based on objective information. It is hard for the Government of Japan to avoid expressing sincere regret concerning those biased recommendations. The Government of Japan requests the Special Rapporteur to read carefully the details of this document provided below.

Last December, the Government of Japan provided information as preliminary comments about the Special Rapporteur's document distributed at the press conference regarding his visit for investigation in Japan from 12 to 19 April 2016. In the preliminary comments, the Government of Japan requested that the final report of the Special Rapporteur to be submitted to the Human Rights Council in June 2017 be based on objective facts and analyses and gave governmental views sincerely on the cases pointed out in the document distributed at the press conference. However, it is very regrettable that the draft report was shared without taking into consideration the information provided in the form of comments from the Government of Japan.

The Government of Japan has supported the Special Rapporteur from the time of his visit for investigation in Japan to the preparation of his draft report, and the Special Rapporteur has expressed his gratitude to the Government for the support he received. Despite this cooperation, it would be very regrettable, if the Special Rapporteur issues those recommendations. On this occasion, the Government of Japan would like to stress that there are strong concerns in Japan that issuing recommendations that are not based on objective facts or analyses but on hearsay information or assumptions as UN documents degrades significantly the authority of the UN Human Rights Council.

The Government of Japan intends to continue dialogues with the Special Rapporteur in order to facilitate the understanding on the actual situation of Japan. On the other hand, the Government strongly requests the Special Rapporteur to take into consideration the information provided by the Government below in preparing his final report and to refrain from repeating a similar approach in future work.

* Reproduced as received.

1. Partners whom the Special Rapporteur met with during his visit

[Paragraph 2]

The information provided in the paragraph is not accurate. The sentence in paragraph 2 "During his visit, the Special Rapporteur met with …the State Minister of Justice…." should be replaced as follows: "During his visit, the Special Rapporteur met with …the State Minister of Justice **who is also the State Minister of the Cabinet Office**…."

This is because State Minister of Justice Moriyama is also the State Minister of the Cabinet, who is responsible for the Specially Designated Secrets Act.

Please modify the last sentence in paragraph2 by adding "the Personal Information Protection Commission," which is one of the organizations the Special Rapporteur met on April 15, 2016. Our suggestion is as follows, "He also met representatives from Cabinet Intelligence and Research Office, … , **and** the Ministry of Education, Culture, Sports, Science and Technology, **and Personal Information Protection Commission**.

2. The suspicion that the Japanese government ordered intelligence community members to monitor a member of civil society who helped coordinate civil society meetings during the visit

[Paragraph 5]

The Japanese government did not attempt to surveille the activities of the person who helped coordinate civil society meetings during the Special Rapporteur's visit to Japan.

3. Media Independence

[Paragraphs 6, 9-14]

Freedom of expression is guaranteed by Article 21 of the Constitution of Japan. It constitutes the political foundation of a democratic nation and is one of the most important fundamental human rights for the people in Japan. It cannot be restricted unjustifiably even by laws. In Japan, freedom of expression is fully guaranteed.

The Special Rapporteur expresses concerns on media independence, referring to certain remarks and behaviors of Government of Japan officials and members of the Japanese ruling party. However, freedom of expression including media independence is fully guaranteed by the Constitution of Japan and there is no such fact that Government of Japan officials and members of the Japanese ruling party have put pressure on journalists illegally and wrongfully. Therefore, we cannot support the Special Rapporteur's claims. With regard to the cases where the Special Rapporteur expressed concerns on media independence, most of them seem to be based on hearsay information or assumptions and the Special Rapporteur does not show any verification of the details of related information. The Government of Japan requests that the final report of the Special Rapporteur to the Human Rights Council be based on objective facts and analyses.

The Broadcast Act has been established within a framework based on the autonomy and independence of broadcasters, and it ensures broadcasters enjoy one of the most free media circumstances in terms of such factors as prudence in taking actions for the breach of program rules.

Freedom of expression, including that of press, is one of the fundamental human rights guaranteed by the Constitution of Japan, and the Government of Japan has obviously given every respect for these rights in applying the Broadcasting Act. We find it truly disappointing to see overall descriptions based on an impression that the Government of Japan is not in favor of the freedom of expression, and thus request that the Special Rapporteur make his descriptions accurate and factual.

In addition, the Special Rapporteur emphasizes the existence of such articles as 174 of the Broadcasting Act and 76 of the Radio Act in the context of pressures on media. This is inappropriately described as the final report to the United Nations as it does not reflect our circumstances truthfully on the following points:

The Ministry of Internal Affairs and Communications, has continued to take the view that the suspension of the operations of broadcasting in accordance with Article 174 of the Broadcast Act or the suspension of the operation of radio stations in accordance with Article 76 of the Radio Act in the case that a broadcast was made in violation of Paragraph 1, Article 4 of the Broadcast Act should apply only in very limited circumstances, complying with all the following conditions.

(a) It is clear that a broadcast in violation of the provisions of the laws was aired.

(b) Furthermore, the broadcast harmed public interests and it was contrary to the purpose of the Broadcast Act, and it is necessary to prevent the recurrence of such a broadcast in the future.

(c) In addition to the above conditions, the same broadcaster repeats a similar act, the broadcaster's measures to prevent the cause and recurrence of such a broadcast are insufficient, and the self-regulation of the broadcaster is not expected to ensure broadcasting in compliance with the laws.

Ministry of Internal Affairs and Communications has continued to maintain the opinion that this provision should be administered with very careful consideration, and successive Ministers for Internal Affairs and Communications have made remarks in line with Ministry of Internal Affairs and Communications's conventional view, as well.

We draw your attention to the fact that there are countries that have independent regulatory agencies and specify criminal penalties or fines imposed by administrative agencies on broadcasters in case of breaching program rules and that those penalties or fines have been in practice. In contrast, there are no such criminal penalties or fines in such cases in Japan.

This is because the Broadcast Act has been established within a framework based on the autonomy and independence of broadcasters, and broadcasters are expected to observe the Act independently.

With the abovementioned fact in mind that other countries have put in place even more severe program rules than Japan, the Special Rapporteur's claim that the jurisdiction of Ministry of Internal Affairs and Communications over broadcasting administration gives rise to pressure on the media has no basis in fact.

Freedom of expression is one of the basic human rights guaranteed by Article 21 of the Constitution of Japan, and Article 1 of the Broadcast Act stipulates that one of the purposes of the Act is "to ensure freedom of expression through broadcasting by guaranteeing the impartiality, truth and autonomy of broadcasting."

Furthermore, Article 3 of the Broadcast Act stipulates that "broadcast programs shall not be interfered with or regulated by any person except in cases pursuant to the authority provided for in laws," thus guaranteeing freedom of broadcast program editing.

To be specific, the Broadcast Act includes the following provisions in order for broadcasters to achieve the appropriateness of its broadcast programs.

(a) The broadcaster shall stipulate standards for the editing of the broadcast programs and shall edit the broadcast programs in accordance with such (Paragraph 1, Article 5).

(b) The broadcaster shall establish a deliberative organ for broadcast programs in order to discuss necessary matters for ensuring the appropriateness of the broadcast programs (Article 6).

The Broadcast Act properly ensures freedom of expression and independence in broadcasting within its framework, and the Special Rapporteur's assertion of "a weak system of legal protection" is incorrect.

[Paragraph 13]

The sentence in paragraph 13 "As an example, in January 2017, the Court rejected a ··· the man's right to privacy, given the serious nature of his crimes." should be deleted.

This is because the summary of the order of the Supreme Court quoted by the report is not precise. Firstly, the order did not include the judgment which rejected the argument regarding the 'right to be forgotten'. In addition, the court did not explicitly mention the 'right to know' either.

[Paragraph 17]

Chapter V THE CABINET of the Constitution of Japan stipulates that executive power shall be vested in the Cabinet and sets forth a parliamentary system of government, thus specifying that each Minister as a member of the Cabinet shall be responsible for the administration of areas under the jurisdiction of the Minister.

There is remarkable technological innovation along with vigorous international competition in the field of information and communications, in particular, to which a national strategic response is required. Accordingly, a structure in which the Minister is responsible for promptly executing administrative matters under the Ministry's exclusive system to ensure a flexible, integrated, and comprehensive response was introduced.

There was a time when administrative committees were introduced widely in Japan after World War II. However, many of them were abolished in and after 1952 for reasons such as vagueness of their responsibilities.

The idea of establishing an independent regulatory authority covering broadcasting in Japan has been strongly opposed by the representatives of the Japan Commercial Broadcasters Association, stating that it would be difficult to establish an organization irrelevant of political interference and that the establishment might strengthen regulation over broadcasters.

The ideal state of broadcasting administrative organizations varies with the circumstances of each country, and in that regard, the Special Rapporteur's assertion that "Under international standards, broadcast regulation should be conducted by an independent third-party actor" needs to be reviewed since there are no such global standards.

And we are aware that many countries have regulations similar to program rules specified by the Broadcast Act of Japan.

As we mentioned earlier, there are countries that have penalties or fines on broadcasters in violation of program rules which Japan does not have, and therefore the Special Rapporteur's criticism over our legal framework is groundless.

[Paragraph 19]

We are aware that there are countries that have independent regulatory agencies and specify criminal penalties or fines imposed by administrative agencies on broadcasters in violation of program rules and that those penalties or fines have been in practice. In contrast, there are no such criminal penalties or fines with respect to cases in violation of the program rules in Japan.

This is because the Broadcast Act has been established within a framework based on the autonomy and independence of broadcasters, and broadcasters are expected to observe the Act independently.

The Government of Japan does not have any information which underpins the Special Rapporteur's assertion that "the possibility of government interference based on content or affiliation" "looms as a threat over the media, possibly deterring investigations that could run afoul of political sensitivities," and in fact there were no cases in which Article 174 of the Broadcast Act or Article 76 of the Radio Act were applied as a result of a violation of Article 4 of the Broadcast Act.

[Paragraph 20]

From the viewpoint of ensuring freedom of expression, the Broadcast Act rules freedom of program editing by stipulating that "broadcast programs shall not be interfered with or regulated by any person except in cases pursuant to the authority provided for in laws," thus forming a mechanism to achieve the appropriateness of broadcast programs according to the autonomy and independence of broadcasters.

Therefore, broadcast programs are to be edited by broadcasters on their own responsibility, and broadcasters are to comply with the Broadcast Act independently and autonomously.

With regard to the program rules specified in Paragraph 1, Article 4 of the Broadcast Act, broadcasters are to determine whether their broadcast programs comply with the program rules first.

From its standpoint as the ministry with jurisdiction over the Broadcast Act, Ministry of Internal Affairs and Communications has been taking the view that it should apply the Broadcast Act, if necessary, with very careful consideration so as not to limit legitimate freedom of expression.

The Broadcasting Ethics & Program Improvement Organization (BPO) was voluntarily established by Japan Broadcasting Corporation (also called NHK) and the Japan Commercial Broadcasters Association (JBA) in July 2003 in order to act promptly and precisely from the standpoint of an independent third party, and to contribute to the enhancing of broadcasting ethics and accurate broadcasting. Ministry of Internal Affairs and Communications recognizes that the activities of BPO are in any case conducted as a part of the autonomous efforts of broadcasters, and therefore, broadcasters are ultimately responsible for their broadcast programs regardless of any decisions made by the BPO.

Meanwhile, from its standpoint as the Ministry with jurisdiction over the Broadcast Act, Ministry of Internal Affairs and Communications has continued to take necessary measures.

It is clear that BPO, a private entity that broadcasters have voluntarily set up, cannot make any interpretation of the Broadcast Act in a legally binding way, and we are not aware of any cases where private entities do so in other advanced economies either. Also, as we stated earlier, it is inappropriate to have an independent regulatory body in broadcasting in Japan's situation.

With regard to measures that involve administrative guidance, Ministry of Internal Affairs and Communications has been carefully considering each individual circumstance before taking action.

[Paragraph 21]

The remarks of the Minister for Internal Affairs and Communications in the Budget Committee of the House of Representatives on February 8, 2016 were made as a response to a question on the possibility of application of provisions relating to the business suspension order stipulated in Article 174 of the Broadcast Act or the operation suspension order stipulated in Article 76 of the Radio Act in the case that a broadcast was made in violation of Paragraph 1, Article 4 of the Broadcast Act. The minister's response was an explanation of Ministry of Internal Affairs and Communications' conventional

interpretation of the framework of the Act. A similar response had been made under the regime of the Democratic Party of Japan as well.

Past Ministers for Internal Affairs and Communications responded similarly from the viewpoint of the continuity of administration, and the remarks of Ms. Sanae Takaichi, Minister for Internal Affairs and Communications were not different from those of past Ministers.

It should be noted that there were no cases in which Article 174 of the Broadcast Act or Article 76 of the Radio Act were applied as a result of a violation of Article 4 of the Broadcast Act.

In any case, the Broadcast Act has a framework based on the autonomy and independence of broadcasters, and broadcast programs should be edited by broadcasters at their own responsibility in accordance with the Broadcast Act.

Moreover, we would reiterate that Ministry of Internal Affairs and Communications has long been of the opinion that in case of a violation of Article 4 of the Broadcast Act Article 174 of the Broadcast Act and Article 76 of the Radio Act should be administered with very careful consideration.

[Paragraph 22-24]

The Special Rapporteur expresses concerns on media independence, referring to certain remarks and behaviors of Government of Japan officials and members of the Japanese ruling party. However, freedom of expression including media independence is fully guaranteed by the Constitution of Japan and there is no such fact that Government of Japan officials and members of the Japanese ruling party put pressure on journalists illegally and wrongfully.

[Paragraph 25]

Since the remarks of the Ministry for Internal Affairs and Communications were made in the Diet on February 8, 2016, some media houses have reported that the resignation of broadcasters and commentators from long-term positions is associated in some way with the remarks. We understand that the program reorganization, including the departure of certain broadcasters, had been decided before the opening of the Budget Committee in February. Therefore, references to an environment hostile to or fearing the consequences of criticism of the Government are irrelevant.

[Paragraph 26]

NHK is Japan's public broadcaster funded by reception fees, which are paid by every household with a television set. From this point of view, some operations of NHK are subject to approval from the Diet, which is composed of national representatives. For example, the members of the Board of Governors are appointed by the Prime Minister with the consent of the Diet. Furthermore, NHK's budget, which is submitted by the Minister for Internal Affairs and Communications with the Minister's opinion attached, should be approved by the Diet.

Therefore, the line which states "the Diet appoints the members of NHK's Board of Governors" is a factual error.

We understand that similar systems exist in other countries. For example, in the United Kingdom, we are aware that the Queen is to appoint the members of the BBC Trust in accordance with the recommendation of the Government, and in France the budget of French public broadcasting requires approval from the Parliament and some members of the Council of Administration are designated/nominated by the Parliament or the Government.

Meanwhile, the Broadcast Act has a framework which respects the autonomy and independence of broadcasters, and, under the framework, those broadcasters edit programs on their own responsibility.

Accordingly, we understand that NHK as well as other broadcasters are to edit programs on their own responsibility and independently and autonomously observe the Broadcast Act.

The Special Rapporteur's assertion that NHK's lack of independence and the Government's pressure influences programs and media selection are not based on a proper understanding of the situation.

Out of the Special Rapporteur's reference to the interview with a certain NHK employee, the allegation that NHK had conducted an internal investigation and that it had not made public its results is not true as we checked with NHK that it had never conducted such an internal investigation. We would be disappointed if the Special Rapporteur should unilaterally publicize to the United Nations his report, which is critical of Japan's media environment based on misunderstood information, and thus we request its review.

[Paragraph 27]

The Special Rapporteur expresses concerns on media independence, referring to certain remarks and behaviors of Government of Japan officials and members of the Japanese ruling party. However, freedom of expression including media independence is fully guaranteed by the Constitution of Japan and there is no such fact that Government of Japan officials and members of the Japanese ruling party put pressure on journalists illegally and wrongfully.

The Special Rapporteur's assertion that "the pressures on the broadcast media have a definite spillover effect on print" is not true, because the interpretation and application of the Broadcast Act do not exert any pressures over broadcasters, and the print and broadcast media have been active independent of each other in Japan. We request that a review be conducted of assertions based on factual errors.

[Paragraph 65]

Freedom of expression is guaranteed by Article 21 of the Constitution of Japan, and Article 12 and Article 13 of the Constitution respectively specify that "The freedoms and rights guaranteed to the people by this Constitution shall be maintained by the constant endeavor of the people, who shall refrain from any abuse of these freedoms and rights and shall always be responsible for utilizing them for the public welfare," and "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs." Furthermore, Article 1 of the Broadcast Act reads, "The purpose of this Act is to regulate broadcasting so as to conform to public welfare and to achieve its sound development."

Article 4 of the Broadcast Act was established in light of the purpose of the provisions of the Constitution.

We are aware that many countries have regulations similar to program rules specified by the Broadcast Act of Japan and that there are countries that specify criminal penalties or fines imposed by administrative agencies on broadcasters in violation of program rules and that those penalties or fines have been imposed in practice. In contrast, there are no such criminal penalties or fines with respect to cases in violation of the program rules in Japan.

The reason is that the Broadcast Act has been established within a framework based on the autonomy and independence of broadcasters, and we expect broadcasters to observe the Act under the framework.

Therefore, we consider that the program rules similar to those of other countries specified in the Broadcast Act are necessary, and we do not agree with the recommendation of repeal of Article 4 and of the Government getting itself out of the media regulation business.

With regard to the recommendation on the independent regulatory authority, we reiterate that it is not appropriate in light of Japan's situation as for instance it is opposed by Japan's broadcasters themselves. The Government of Japan strongly urges the Special Rapporteur to make recommendations based on the realities and background of the visited countries.

4. Interference in the Communication/Expression of History

[Paragraph 37]

With regards to school education, the Courses of Study (national curriculum standards), which is the standard for the design of the school curriculum based on the law, requires that students should be taught to understand that World War II caused tremendous suffering to humanity at large. Regarding textbooks produced in the private sector, the judgement as to what kind of specific matters to include and how they are described in a textbook is left to the particular textbook publisher as long as the contents are based on the Courses of Study (national curriculum standards) and do not contain errors. In addition, some textbooks do mention the comfort women.

[Paragraph 38]

The information has factual mistakes. In fact, there are about 150 members on the Textbook Authorization Research Council, and among them, about 30 members are in charge of social studies textbooks.

[Paragraph 40]

The information has factual mistakes. In fact, among the junior high school history textbooks used from 2006 to 2011, one textbook contained a description of the comfort women. Moreover, although there were no descriptions of the comfort women in the textbooks used from 2012 to 2015, among the textbooks that have been used since 2016, one textbook contains a description of the comfort women.

Regarding textbooks produced in the private sector, the judgement as to what kind of specific matters to include and how they are described in a textbook is left to the particular textbook publisher as long as the contents are based on the Courses of Study (national curriculum standards) and do not contain errors.

[Paragraphs 41, 42, 69]

Regarding textbooks produced in the private sector, the judgement as to what kind of specific matters to include and how they are described in a textbook is left to the particular textbook publisher as long as the contents are based on the Courses of Study (national curriculum standards) and do not contain errors.

The basic purpose of the textbook authorization is to identify any errors in the textbook descriptions in light of the results of objective academic research and appropriate materials at the time of the authorization, and the authorization is conducted based on the Courses of Study (national curriculum standards) and Textbook Authorization Standards. In other words, the textbook authorization is carried out by the Textbook Authorization Research Council based on the results of professional and academic research and deliberation. The results of the examination are utilized as they are by the Minister of Education, Culture, Sports, Science and Technology when judging whether to authorize a particular textbook or not. This authorization mechanism does not allow intervention by government policy or political intent or motivation.

5. The Specially Designated Secrets Act

A. The scope of specially designated secrets designation

[Paragraphs 43, 44, 45]

In the Specially Designated Secrets Act (hereinafter referred to as SDS Act), information designated as SDS is limited to the matters set forth in the appended table of four areas with 23 items. To prevent arbitrary designation, the four areas with 23 items are divided into 55 sub-items in the Standards for Uniform Implementation of the Act on the protection of Specially Designated Secrets, which was formulated based on the opinions of the members of Council for Protection of Information.

As we mentioned above, those 23 items and 55 sub-items stipulated in the Standards for Uniform Implementation of the Act defines the type of information which should be designated as SDS concretely and correctly, which prevent the Japanese government from designating vague and broad information as SDS. Therefore, the comment in the report that the Act contains a vague and broad definition of the matters that can be classified as SDS is not true.

Even before the enactment of the Act, the National Public Service Act required public servants to protect certain information as official secrets. After the enactment of the Act, strictly limited kinds of information among those official secrets are designated as SDS. Therefore, we cannot support the Special Rapporteur's claims that enactment of the Act has led to an expansion of the scope of secrets, preventing information which used to be disclosed from disclosure, or putting in peril the public's right to know.

B. Penalties

[Paragraphs 44, 47, 48]

Information gathering activities performed by journalists are not punished in the Act. The judgment of the Supreme Court of Japan on May 31st, 1978 states, "the patient and persistent persuasion or request to a government official by the press essentially lack illegality and shall be treated as lawful activities in the pursuit of business as long as they are truly for the purpose of news reporting and are generally accepted by society as an appropriate measure, within the entire spirit of the law." In respect of the judgment above, the Act stipulates that the information gathering activities by persons engaged in publishing or news reporting shall be treated as lawful activities in the pursuit of business if they are conducted solely for the purpose of promoting the public interest and when they are not found to have been performed through violation of laws or regulations or by extremely unreasonable means. In other words, the information gathering activities shall be treated as lawful activities in Article 35 of the Criminal Law, and shall not be punished. This judgement also says "the use of extremely unjustifiable ways", which is stipulated in Paragraph 2, Article 21 of the Act, means the ways which impair substantially the personality of an individual who is the object of news gathering activities. This was clearly mentioned in the past Diet discussion.

The official commentary on the Act, which is available online, concretely enumerates the examples of "lawful activities in the pursuit of business" by persons engaged in news reporting as follows: (a) a visit to persons engaged in the duty of handling SDS without any appointment in the early morning or in the middle of the night, (b) repeated attempts of contact by email, phone or direct visits, (c) communication with each other or dining together based on a private relationship, (d) accidental glance at SDS on a screen or in print in a room that one happens to enter, (e) turning over a sheet of paper that had been left blank side up and unattended, taking a glance at or taking a photo of that paper, (f) touching a keyboard to activate a computer on a power saving mode to view a screen which displays data not protected by passwords, (g) interviewing persons who handle SDS or persons who

are closely associated with those who handle SDS, (h) interviewing persons in sections which are closely related to sections handling SDS, (i) interviewing politicians who have come to know SDS, (j) interviewing a family member of persons handling SDS, (k) interviewing employees of eligible contractors which deal with SDS.

Therefore, the Act does not have any negative effect on the activities of journalists. As a fact, though almost two and a half years have passed since the Act has been enforced, we have not recognized any facts that news gathering activities have been daunted by the Act.

The sentence in paragraph 48 "The Special Rapporteur was pleased to hear from officials that the Government does not intend to apply Article 25's harsh penalties to journalists and that the **unknowing** disclosure of information by journalists will not be punished as long as the information is in the public interest and is acquired in the good faith and lawful pursuit of journalism." should be replaced as follows: "The Special Rapporteur was pleased to hear from officials that the Government does not intend to apply Article 25's harsh penalties to journalists and that **any** disclosure of information by journalists will not be punished as long as the information is in the public interest and is acquired in the good faith and lawful pursuit of journalism."

Information gathered by journalists for the sole aim of furthering the public interest is not regarded as penalty subject. It does not matter whether the journalists know the information is SDS or not.

C. The Oversight Mechanism

[Paragraphs 50, 77]

The Board of Oversight and Review of Specially Designated Secrets is established independently in the House of Representatives and in the House of Councilors. During the last year, the committee of the Board in the House of Representatives was held 12 times and the committee of the Board in the House of Councilors was held10 times. To comply with requests from committees through discussion with them, we have disclosed 7 SDSs to the Board in the House of Representatives. Therefore, we consider that the comment that "the committees are left without sufficiently specific information to determine whether the designation of information as secret was appropriate" is incorrect.

The Cabinet must issue the statement to deny the Board's request with the resolution of the Board. This statement has been issued only once in the last 70 years, which shows the difficulty for the government to deny the request from the Diet.

In Paragraph 6 Article 102 of the Diet Law, the Board can request the Head of the Administrative Organ to report the measures taken by the Administrative Organ for the recommendation from the Board.

In the Act, it is provided that the government holds the Council for Protection of Information, which consists of representatives of third parties from the media, judicial circles, academia and public business sectors and takes technical and objective opinions from the members. Also, in the Cabinet Office, the Inspector General for Public Records Management (Information Security Oversight Division), is established to independently and fairly verify and inspect whether Administrative Organs properly designate and terminate SDS, and manage and dispose of administrative documents as well.

Therefore, a multi-layered structure which ensures appropriate implementation of the Act is established.

D. Reaction to the points made by the Board of Oversight and the results of the Review of Specially Designated Secrets

[Paragraph 51]

The Government has explained sufficiently to the Board from the first year of the Act's enforcement, and we will seek further explanation hereafter. In the report from the Board of the House of Representatives issued in 2017, the chairman of the Board, appreciates that the government's actions for the Board have been increasingly positive.

The sentence in paragraph 51 "The boards examined a total of 382 cases in which 10 government organizations designated approximately 189,000 pieces of information as state secrets." should be replaced with the following: "The boards examined a total of 382 SDSs designations which covers 189,000 pieces of SDSs documents".

The figure 382 is a total of SDSs which 10 administrative organs designated at the end of 2014. The figure 189,000 is the number of documents which contain SDSs.

E. Information which does not jeopardize Japan's national security is not designated as SDS

[Paragraphs 73, 74, 75]

In the Act, it is a requirement to designate SDS as Information which would jeopardize Japan's national security if it is disclosed. Thus, information which would not jeopardize Japan's national security if it is disclosed is not designated as SDS.

However, Article 22 stipulates the penalties about disclosures of information as follows considering the citizen's right to know; persons engaged in publishing or news reporting are not penalized even if they disclose SDSs.

Article 24 stipulates that acquirement of SDSs is punished only when the way and the purpose is illicit. This shows that the scope of application of the penalty is narrowed.

Those two articles (Article 22 and 24) are illustrated in the official commentary on the Act and the commentary is available online.

F. Freedom of expression and speech is guaranteed in the Constitution of Japan

[Paragraph76]

Starting with freedom of speech, freedom of expression is a fundamental human right guaranteed in the Constitution of Japan and the Japanese Government takes it for granted that we highly respect these fundamental human rights.

6. Hate Speech

[Paragraph 53]

The sentence in paragraph 53 that states "According to the report, there were 1,152 demonstrations in 29 prefectures across Japan targeting specific races and ethnicities from April 2012 through September 2015" should be modified as follows:"According to the report, there were 1,152 demonstrations in 29 prefectures across Japan held by associations which have been pointed out by the media as having conducted demonstrations with hate speech from April 2012 through September 2015."

This is because the description relating to the demonstrations in the report as targeting specific races and ethnicities is incorrect. The demonstrations were held by associations which have been pointed out by the media as having conducted demonstrations with hate speech.

7. Election Campaigns

[Paragraph 57]

With regard to the election campaign in Japan, the Public Offices Election Act limits the period of election campaigns and establishes certain rules for the means of campaigning so that the election campaign is carried out under the same conditions for fairness in elections.

Restrictions on the election campaigns have been set by law after deliberate discussions among the political parties and the Diet, and by making such efforts from the past, they have been able to formulate the current rules.

The restrictions on door-to-door visits and distributing electoral documents exemplified in the draft report are restricted by the following reasons:

(a) door-to-door visits are likely to become a hotbed for activities such as acquisition and profit induction, and have the harmful effect of disturbing the peace; and

(b) the use of unlimited documents increases expenses and labor, and leads to unfairness due to differences in economic power.

The Supreme Court has decided that restrictions on election campaigns in our country are necessary and reasonable to ensure the freedom and fairness of the elections and that those restrictions do not violate provisions on guarantee of suffrage and freedom of expression in the Constitution of Japan. The Supreme Court has also decided that the restrictions do not violate Article 19 and Article 25 of the International Covenant on Human Rights on Civil and Political Rights. For this reason, the Special Rapporteur's indication of "unnecessary and disproportionate" restrictions is inappropriate.

Although the Special Rapporteur pointed out that the Human Rights Committee has called our country's attention to the need to repeal legislation imposing unreasonable restrictions on political campaigning, this call to attention had been deleted in the concluding observations on the sixth periodic report of Japan of 2014, which is the most recent concluding observations of the Committee, in response to the countermeasures of the Japanese government in the sixth periodic report of 2012. The Special Rapporteur should take full account of such circumstances.

Regarding political activities, they are basically free as long as they do not involve a campaign movement.

In addition, as we stated earlier, the Special Rapporteur's assertion that political fairness stipulated in the program rules has been putting pressure on Japan's journalism is not true as it is based on a misunderstanding of the careful application of the Broadcast Act and its basic framework of autonomy and independence of broadcasters, and therefore we request deletion or correction of the related descriptions.

[Paragraph 71]

As mentioned in the paragraph referring to the 57, the Special Rapporteur's indication of "unnecessary and disproportionate" restrictions is inappropriate, and restrictions on election campaigns in our country do not violate international human rights law. We strongly urge the Special Rapporteur to delete this description.

8. Demonstrations

[Paragraphs 58, 59]

The report pointed out that there are "concerns about unnecessary restrictions on protest"; however, in Japan, freedom of expression is widely guaranteed to the maximum extent, and there are no grounds for such concerns.

Although the report also pointed out that there are reports on "disproportionate restrictions on protest activities taking place in Okinawa" and "excessive use of force and multiple arrests," these allegations are not based in fact. The authorities have merely taken legitimate and necessary measures only in such cases when any illegal activities are confirmed or when there is a risk of such activities. As for the protest activities taking place in the Henoko district in Nago City and the Takae district of Higashi Village in Okinawa Prefecture, some protesters commit obstructive behaviors that are dangerous and illegal such as going under a car, running out in front of a moving car, or parking their cars in a manner that obstructs other vehicles. Their behaviors create dangerous situations that will possibly lead to traffic accidents. In addition, during the protests, there have been many cases in which the performance of official duty is obstructed, including instances where the protesters assaulted police officers on duty maintaining public order.

Under such circumstances, the police authorities take minimum required security measures in an appropriate manner, in light of ensuring safety and maintaining orders on the ground. The police have never used excessive physical force. If illegal acts are confirmed in the process, we appropriately address the situations according to relevant laws and regulations by taking necessary measures including making arrests.

The reference to "credible reports of excessive use of force and multiple arrests" is incorrect. There are no facts that the Japan Coast Guard has committed excessive use of force against protesters, or arrested protesters with regard to public demonstrations at the sea in Henoko, Okinawa. (There is only one case that Japan Coast Guard officers arrested a protester but not with excessive use of force. He was initially captured by the U.S. Military Police as he invaded into the restricted area of Camp Schwab and handed over from them based on the "Act to Provide for the Special Criminal Act Pertaining to the Enforcement of the Agreement under Article VI of the Treaty of Mutual Cooperation and Security between Japan and the United States of America, Regarding Facilities and Areas and the Status of United States Armed Forces in Japan" on April 1, 2016.)

The Japan Coast Guard never denies safe and legal public protests. Almost all protesters undertake safe and legal protest activities. Nevertheless, there has been behavior by some protesters that cannot be overlooked, such as invading areas of the sea that are restricted by law, sailing *zigzag* at high speed, diving into the sea in the vicinity of construction sites in such a dangerous manner that it could lead to a fatal accident, and clinging to workboats.

Accordingly, the Japan Coast Guard has implemented minimum measures necessary to restrain dangerous or illegal acts in order to protect the lives of and prevent injury to the protesters and the construction staff. Therefore it is not the excessive use of force.

As for the reference to "concerns about the recording of protesters," the police do make video recordings as a part of police activities, but this is merely for the legal and proper execution of duties to preserve necessary evidence, and is conducted only in cases where illegal acts occurred or such acts are highly likely to happen. The police do not record every single protest, nor do they intend to record the substance of protests or conduct investigations on their participants. We have seen many incidents where protesters obstruct official duties by assaulting a police officer who is patrolling on the site. When such an illegal act happens, the police give repeated warnings and take necessary measures including the recording of video footage.

There are no facts pertaining to excessive use of force against journalists filming the protests.

The reported case is probably the case on January 20, 2019. In this case, the protest boat ignored repeated instructions and warnings by the Coast Guard officers and committed dangerous acts such as approaching a construction site. As such, the Coast Guard officers moved the protest boat to a safe place to secure the safety of the protest boat and construction workboats.

At that time, a woman on the protest boat was standing in an unstable position to take a video while holding a large camera with both hands. Part of her body even protruded from the boat. It was such a dangerous situation that might lead her to falling into the sea. As such, the Coast Guard officer kept her body to prevent the woman from falling into the sea. There was no fact that the officer used excessive force against the woman.

In this process, the Japan Coast Guard found no injury on her, and received no claim that she was injured from her.

Also, the Japan Coast Guard was not charged with this case.

As for the "concerns on the failure to deal with those who interfere with protests from the right-wing of the political spectrum," although the details of these concerns are not entirely clear as the topic was not touched upon at the meeting with the Special Rapporteur, generally speaking, the police takes appropriate security measures in regard to all protests in light of preventing any problematic incidents and from the perspectives of neutrality and equality, regardless of protester's claims.

As for the reference to "allegations of surveillance of the Muslim community," we believe this is based on a factual misunderstanding. In fact, the police do not monitor the Muslim community. It is true that the police collect information on Islamic extremists, as Japan faces the threat of terrorism by Islamic extremist organizations as evident from the series of recent overseas incidents involving Japanese citizens. However, this does not mean that the police conduct surveillance of the Muslim community.

Moreover, although the report says "I shared these concerns with members of the National Police Agency," the Government of Japan requests to note that the National Police Agency does not have any concerns on this particular claim, as the claim is based on factual misunderstanding. We explained this to the Special Rapporteur at the meeting held on April 18th last year.

As for the point that "careful review processes must be in place to avoid abuses," the Prefectural Police and the Japan Coast Guard have a mechanism for review of their measures, and have established a careful review process.

To ensure the democratic administration and the political neutrality of the police, a Prefectural Public Safety Commission, consisting of three or five external experts, is established in each prefecture. They supervise the Prefectural Police from the perspective of a third-party. The Prefectural Public Safety Commission receives document-based complaints against police officer's performance, handles them faithfully, and informs the complainants of results according to the Police Act.

When the Prefectural Public Safety Commission receives the complaint, they instruct relevant departments of the Prefectural Police to investigate the facts and take measures based on the results.

In the case that the Prefectural Public Safety Commission receives a complaint by phone or e-mail, the Prefectural Police also handles them faithfully in conformity with relevant regulations required by the Police Act, and utilizes them for improving their service.

When any illegal or unjust act by a police officer is confirmed in the process of an investigation of complaints, the inspection department of which manager is appointed by the National Public Safety Commission, which is also a third-party organization, makes investigations and imposes disciplinary punishment on the officer(s) concerned in light of the situation. The department informs the Prefectural Public Safety Commission of the results of the investigation and any punishment to be administered. In this process, the Prefectural Public Safety Commission may give the Prefectural Police concrete instructions on the investigation method or the details of the punishment if necessary.

As mentioned above, the Prefectural Public Safety Commission, supervises complaints handling by the Prefectural Police as well as investigations/punishment by the inspection department as a third-party organization. Therefore the implementation of the careful review process of the police is fully guaranteed to take place.

The Japan Coast Guard has a mechanism to review its measures, and has established a careful review process.

For example, the Japan Coast Guard accepts opinions on its Web site, and there is a mechanism for listening to a wide range of public opinion to accept advice and receive complaints about Coast Guard administration.

When the Japan Coast Guard receives a complaint, the Japan Coast Guard investigates the reported fact and reviews it. Additionally it is possible to file a criminal charge or accusation against action taken by the Japan Coast Guard based on the Code of Criminal Procedure. It will be decided according to the investigation whether the Public Prosecutor's Office indicts our agency staff in this case. If the Public Prosecutor's Office decides not to prosecute and an objection is made, it is possible to appeal and request a ruling from a Prosecution Committee formed of third parties.

[Paragraph 60]

Comment on L.4 – L.6

With regards to the charges, the place where Mr. Yamashiro assaulted an official of the Okinawa Defense Bureau was not at Camp Schwab in the Henoko area of Nago but on a construction road used for relocation of the helicopter landing zone in the Northern Training Area of the U.S. forces.

He was charged with obstructing the public duty of an official of the Okinawa Defense Bureau working at the site and inflicting injury on the official that required two weeks' treatment.

In addition, he was also charged with obstructing relocation work forcibly by piling up approximately 1,500 concrete blocks in front of the construction gate of Camp Schwab in the Henoko area of Nago.

Comment on L.8 – L.12

Mr. Yamashiro was arrested and detained not for public protest or dissent but for his illegal behavior including the assault on the official.

The police have arrested Mr. Yamashiro three times since October 17, 2016. Apart from the on-the-spot arrest, the other two arrests were conducted with arrest warrants issued by a court judge who confirmed that there was probable cause enough to suspect that he had committed crimes and determined that it was necessary to arrest him.

The on-the-spot arrest was conducted in accordance with Article 213 of the Code of Criminal Procedure, and the arrests based on arrest warrants were conducted in accordance with Article 199 of the Code.

With regards to the detention of Mr. Yamashiro, the court found there was probable cause to suspect that he has committed crimes and necessity for detention, and issued the detention warrants. Furthermore, after the prosecution, the court found there was special necessity to continue the detentions, and decided to extend the period.

The detentions were conducted in accordance with Article 207 and Paragraph 1, Article 60 of the Code of Criminal Procedure. The renewal of the detentions period was conducted in accordance with paragraph 2, Article 60 of the Code of Criminal Procedure.

As described above, all the concerned authorities responded to Mr. Yamashiro's illegal activities appropriately and in accordance with relevant laws and regulations, fully respecting due process.

[Paragraph 72]

Comment on L.5 – L.7

In Japan, freedom of expression, including the right to hold demonstrations, is guaranteed by Article 21 of the Constitution of Japan. It constitutes the political foundation of a democratic nation and is one of the most important fundamental human rights of the citizens, and therefore cannot be restricted unjustifiably even by law. The government does not impose penalties on protesters if they protest or dissent in accordance with relevant laws and regulations.

Although the details of the concern about "the pressures placed on public protest in Okinawa" is not entirely clear, under circumstances of public protest, the police take minimum required security measures in an appropriate manner in light of ensuring safety and maintaining orders on the ground. The police have never used excessive physical force. If illegal acts are confirmed in that process, we appropriately address the situations according to relevant laws by taking necessary measures including making arrests.

[Paragraph 76]

The words in paragraph 76 "the courts." should be deleted.

This is because that court in Japan is an organization to apply law to specific cases, not to declare supportive policies and statements.

9. Conclusion

The Government of Japan has consistently upheld basic values such as fundamental human rights, freedom and democracy including freedom of expression and made ceaseless efforts toward their realization. The Government of Japan intends to continue dialogues with the Special Rapporteur in order to facilitate the understanding on the actual situation of Japan and requests once again the Special Rapporteur to take into consideration and reflect the aforementioned information provided by the Government of Japan in preparing the final report. The Government of Japan believes that only this will lead to foster a trusting relationship between us toward the guarantee of freedom of expression.

United Nations A/HRC/35/22/Add.6

General Assembly

Distr.: General
7 June 2017

English only

Human Rights Council
Thirty-fifth session
6-23 June 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Turkey: comments by the State

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the comments by the State on the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Turkey.

GE.17-09208(E)
1709208

Please recycle

Report of the Special Rapporteur the promotion and protection of the right to freedom of opinion and expression on his mission to Turkey: comments by the State*

Response to recommendations

The Government of the Republic of Turkey notes the cooperation of Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression with Turkey in the context of his mandate. After studying the Report which was prepared by the Special Rapporteur's office following his mission to Turkey from 14 through 18 November 2016, the Government of the Republic of Turkey would like to highlight the following:

At the outset, the Government wishes to remind that FETÖ/PDY (Fetullahist Terrorist Organization/Parallel State Structure) is an armed terrorist organization established by Fetullah Gülen which aims to suppress, debilitate and direct all the Constitutional institutions, to overthrow the Government of the Republic of Turkey and to establish an oppressive and totalitarian system through resorting to force, violence, threat, blackmailing and other unlawful means. Accordingly, the references to the said group in the Report such as *"Gülen movement"* (Paragraph 26), *"Gülenist movement"* (Paragraph 31 and Paragraph 56), Gülenists (Paragraph 71) should be corrected as FETO (Fetullahist Terrorist Organization) or "members of FETO" where necessary.

The Government further would like to underline that PKK is a vicious terrorist organization, which is included in the lists of terrorist entities of the EU as well as USA and many other countries in the democratic world. For decades, Turkey has been countering PKK terrorism which claimed thousands of lives of innocent people and violated the fundamental rights and freedoms of people; first and foremost, the right to life. Accordingly, it is deplorable that the terrorist nature of this organization and the grave threats that it poses in Turkey have not been duly reflected in the Report (Paragraph 5, Paragraph 41, Paragraph 55, Paragraph 57).

Introduction

It should be reminded that freedom of expression and the media constitutes one of the foundations of Turkish democracy. The Constitution guarantees the right to express and disseminate thoughts and opinions without interference by official authorities as well as the freedom of the media. It provides that no one shall be blamed or accused because of his/her thoughts and opinions.

While acknowledging the serious nature of the security challenges that Turkey faces in recent years, the Report cites in Paragraph 7 unsubstantiated, generic and vague claims such as *"legal and institutional pressures"* and *"squeezing of civil society space"*, *"radical backsliding from Turkey's democratic path"*. Turkey remains resolved to further align its legislation and implementation with the European Convention on Human Rights (ECHR) and the jurisprudence of the European Court of Human Rights (ECtHR) with a view to further strengthening fundamental rights and freedoms, including freedom of expression and the media. Those claims set forth in Paragraph 7 are neither appropriate nor in line with the realities on the ground.

The Government would further like to inform that the criminal terrorist acts perpetrated by FETO elements during the attempted coup on 15th July 2016 caused the deaths of 249 persons, including 181 civilians and the figures in the Report should be corrected accordingly. Legislation

* Reproduced as received.

Paragraphs 14-18 claim that "Article 7 of the Law No: 3713 (cited in the Report as 37137 mistakenly) permits punishment of those who make "propaganda" for a terrorist organization, but key terms are left undefined and other legislation include vague terms on the issue".

The Government wishes to inform that the elements of the offence set out in Article 7 § 2 of the Law No: 3713 (Anti-Terror Law) were redefined on 30 April 2013. As per the amendment, the act of making propaganda of terrorist organizations by justifying or praising or inciting their methods has been recognized as an offence only if they contain violence, force or threat, which is in compliance with the case-law of the ECtHR.

Thus, the nature of the offence has been further concretized and the provision has narrowed in order to bring the judicial practice further in line with the case-law of the ECtHR. Accordingly, peaceful enjoyment of freedom expression in this respect will not any more constitute a crime.

The Article reads before and after the amendment as follows:

Art. 7 § 2 (Former Version)	**Art. 7 § 2 (Amended Version)**
Anyone who makes propaganda of a terrorist organization shall be sentenced to imprisonment for a term of one to five years (...)	Anyone who makes propaganda of a terrorist organization by justifying or praising or inciting the terrorist organizations' methods which contain violence, force or threat shall be sentenced to imprisonment for a term of one to five years (...)

Paragraph 18 sets forth the claim that "Article 299 of the Penal Code criminalizes defamation of the President, with sentences of one to four years in prison and reports indicate that the Justice Ministry has initiated up to two thousand defamation cases for 'insult' of the President".

The Government wishes to highlight that the Article 299 of the Penal Code was adopted in light of international conventions to which Turkey is a party. There are similar provisions in penal codes of other Council of Europe member states. Freedom of expression is one of the basic tenets of a democracy based on the rule of law. However, this freedom does not include insult and statements that spread, incite, promote or justify hatred or expressions constituting hate speech. Recent acts constituting defamation against the President are mostly in the form of vulgar and disgraceful swearing and are not based on facts or criticism. Most of these cases also concern hate speech. These statements have nothing to do with freedom to expression. In July 2016, the President, as a clear sign of his good intentions and for encouraging reconciliation in the society, decided to withdraw cases of insult against him and his family except some very serious ones.

It is claimed in **Paragraph 20** that "Law no.5651, The Internet Law, allows the Government to restrict access to Internet content and telecommunications network. Amendments in March 2015 introduced Article 8(A), which expands the power of the Telecommunications and Communication Presidency (TIB) to order the blocking of websites on vaguely defined grounds and without prior court approval."

The Government wishes to highlight that Law numbered 5651 is not about telecommunications network and its restrictions. Amendments in March 2015 introduced Article 8(A) which aimed to ensure that protective measures can be taken with respect to

violations that can occur in the Internet within limited time involving one or several of the grounds of protection of national security and public order.

In emergency cases, removal of content and/or blocking of access decisions under Article 8/A are taken by the Information and Communication Technologies Authority (ICTA) upon the request of the Prime Ministry or relevant Ministries and decisions are submitted to the court for approval within twenty-four hours. In these cases, the judge declares her/his decision within forty-eight hours and otherwise the decision is revoked automatically.

In **Paragraph 21,** it is stated that "as of 2015, the government had used the blocking measures, along with related court decisions, to block over 110,000 websites and over 16,500 URL's." The Government wishes to point out that the Report refers to speculative data gathered from unofficial resources. The proceedings regarding blocked illegal contents are related with criminal issues (approximately 99.5%) such as child sexual abuse, obscenity, prostitution, etc.

In **Paragraph 21,** it is also stated that "in requesting access bans, the office of the prime minister submits a formal request to ICTA, which must forward the request to a Criminal Peace Judge within a 24-hour period. If approved, all relevant service providers are obligated to acquiesce to the decision. There is no appeal following a court order." The Government would like to clarify that general appeal procedures are valid for the said court decisions and also option of individual application to the Constitutional Court is available. It is also not true that "the ICTA requires providers to use government-approved filtering systems." Previously, according to the "Regulation On Internet Public Use Providers", only internet cafes required to use approved filtering system. This obligation has been lifted with the amendment made in the regulation.

Regarding **Paragraph 22**, it should be stressed that Article 4 of the Internet Law is only about the responsibility of the content providers, not "taking down content".

State of Emergency

On the night of 15 July, upon the instruction of the founder and leader of the FETÖ/PDY, Fetullah Gülen, and in line with the plan approved by him, a group of terrorists in uniforms within the Turkish Armed Forces attempted an armed coup against the Turkish democracy for the purpose of overthrowing the elected president, Parliament and Government together with the Constitutional order. Taking the existing condition into account and in order to fight effectively against the FETÖ/PDY in line with the recommendation of the NSC, by the decision of the Council of Ministers, a nationwide State of Emergency has been declared as from 21 July 2016 for three months, pursuant to Article 120 of the Constitution and Article 3/1-b of the Law No. 2935 on State of Emergency.

With a view to ensuring continuity of the effective implementation of measures for the protection of Turkish democracy, the principle of the rule of law, as well as the rights and freedoms of the citizens, the Council of Ministers decided to extend the State of Emergency, lastly until mid-July 2017.

In this context, Turkey resorted to the right of derogation from the obligations in the European Convention on Human Rights (ECHR) and International Covenant on Civil and Political Rights (ICCPR). Notifications of derogation from Convention obligations were submitted to the Council of Europe in accordance with Article 15 of the ECHR and to the Secretariat of the United Nations in accordance with Article 4 of the ICCPR, concerning the rights permitted by the Conventions. This includes Article 19 of the ICCPR, concerning freedom of expression, which is not listed among the non-derogable articles.

In this process, Turkey is fully aware of its obligations under international conventions and acts in full respect for democracy, human rights, the principle of rule of law. Due respect is shown to fundamental rights and freedoms and the of rule of law is strictly observed. The principles of "necessity", "proportionality" and "legality" have been sensitively complied. The Government would also like to underline that while taking the measures under Article 15 of the ECHR, the State parties naturally continue to be subject to the supervision of the ECtHR.

A Decree with Force of Law (Decree Law) is a legal measure permissible in the context of State of Emergency in Turkey and they are approved by the Parliament. By the Decree Laws issued within the scope of the State of Emergency, measures have been taken in proportion to the present situation that the administrative authorities are faced with, to the extent necessitated by the situation and in pursuit of a legitimate aim which is national security. Legal remedies are available.

FETÖ/PDY is an atypical armed terrorist organization which is scarcely encountered in the world, unlike PKK or DAESH. In this perspective, the required measures are taken with a view to averting the organization's strength within the state. In the meantime, the scope of the Decree Laws issued in this respect has been limited to the terrorist organizations in order not to interfere with the rights and freedoms of others.

The Government wishes to underline that it was due to increasing threats against the survival of the state and the nation that made inevitable to take measures under State of Emergency since 21 July 2016.

State of Emergency measures are constantly reviewed. In this process, Turkey maintains a close dialogue with the Council of Europe organs and mechanisms. With the existing domestic remedies, to date, over 300 institutions (including 187 associations, 21 foundations, 92 private education institutions, 5 radio-TV channels, 17 newspapers and 1 private health institution) have been reopened and more than 30 thousand public employees have been reinstated. With the decree laws issued on 23 January 2017, further measures have been introduced. For instance, the Inquiry Commission on State of Emergency Measures has been established as a domestic legal remedy, to address applications in particular against dismissals and closure of associations, institutions including those of media which were carried out as listed in relevant decree laws. Decisions taken by this commission are subject to judicial review. Furthermore, the maximum duration of police custody has been reduced from thirty days to seven days. Lastly, the provision enabling public prosecutors to impose restrictions up to five days for the persons in police custody on consulting their lawyers has been abolished.

In this context, the claims such as in the **Paragraph 28** that *"the state of emergency decrees adopted in the aftermath of the coup attempt are far reaching"* are neither appropriate nor reflect the realities.

So called "Attacks on the Media and right to information"

The Government wishes to stress that the activities of many of outlets cited in the Report were ceased due to their established links with terrorism and terrorist organizations. They are subject to criminal investigations. In the context of these investigations, a number of Criminal Magistrates' Offices indicated that those press and media organizations made publications as per instructions of the founder and the executives of terrorist organizations in order to achieve their illegal goals.

Certain individuals who have been working as journalists or media workers are currently charged with serious crimes - such as being a member of, or supporting an illegal or armed terrorist organization. The criminal investigations and prosecutions are conducted against the concerned persons for their activities which are defined as an offense pursuant to the Turkish criminal legislation. The related investigations are not due to their journalistic work but due to their support and link to the terrorist organization and other non-journalistic activities, or using their profession in the service of terrorist activities.

In **Paragraph 36**, as to the case of daily Cumhuriyet, the Government refers to the fact that it has submitted comprehensive information on the nature of proceedings against the said newspaper to the UN Working Group on Arbitrary Detention per latter's communication dated 2 February 2017 (Reference: 2017/TUR/Case/2). For the ease of reference, it is annexed herewith.

The claims in the **Paragraph 36** that *"the legal actions taken against the newspaper Özgür Gündem targeted both its regular staff and people who had loose connection to the newspaper, such as its advisors or symbolic editors, many of whom are intellectuals*

wanting to make a contribution towards solving the Kurdish issue through dialogue" are at odds with the realities. There were previous criminal investigations concerning Özgür Gündem and the charges included making terrorist propaganda for the PKK terrorist organization. The newspaper was closed down with Decree Law 675.

In **Paragraph 37**, it was asserted that Silivri Prison housed an estimated thirteen thousand prisoners. It is misleading that a single prison in Silivri hosts thirteen thousand inmates. The said facility is a combination and a general campus of ten prisons and detention houses. As of 16 November 2016, the prison visited by the Special Rapporteur hosted only four hundred and fifty six prisoners.

Also in **Paragraph 38** it is claimed that "*on 28 September 2016, another 12 television and 11 radio stations (owned or operated by members of the Kurdish or Alevi minorities) were shut down, without the involvement of the judiciary or any review procedure, on charges that they spread "terrorist propaganda*". The Government wishes to inform that Turkish citizens of Kurdish or Alevi origin are not minorities in Turkey. Minority rights in Turkey are regulated in accordance with the Lausanne Peace Treaty of 1923, under which Turkish citizens belonging to non-Muslim minorities fall within the scope of the term "minority".

The constitutional system in Turkey is based on the equality of all individuals without discrimination before the law, irrespective of "language, race, colour, gender, political opinion, philosophical belief, religion and sect, or any such consideration" (Art. 10, Constitution). All citizens, regardless of whether they are recognized as a minority, enjoy rights and freedoms also in respect of their origins.

Furthermore, these televisions and radio stations mentioned in **Paragraph 38** were shut down in September 2016, as their affiliation and/or connection with terrorist organizations were proven. The shutdown decisions were taken not because of the owners of the televisions or radio stations but because of the violations.

Restrictions on Internet

With regard to **Paragraphs 48-54**, it should be emphasized that the Turkish national legislation, in the first place, makes use of a "notice and take down" procedure regarding internet governance, in line with the principle of proportionality. Under this procedure, the content and hosting providers can be first contacted to demand the removal of a particular content. It is also possible to apply to the court which may order the removal of the content on the grounds of inter alia national security and public order, prevention of crime or protection of public health. In cases in which the content removal is not technically possible, the court may order, as a last resort, blocking access to the internet site which publishes the content in question.

Only as an exception, in cases where delay may cause irreversible damage, the national legislation authorizes the Prime Ministry to take any necessary measure on the aforementioned grounds and to notify the Information and Communication Technologies Authority (ICTA) for implementation. The decision is conveyed to access and hosting providers which are to implement it within two hours. Then decision is submitted for the approval of the judge within 24 hours. The judge shall announce his/her decision within 48 hours. If not, the restriction shall be automatically lifted.

The main reasons behind resorting to the measure of access blocking derives from the technical difficulties in removing a particular content from most of the internet sites. It is technically not possible to block access to a particular content in internet sites in "https" format. In these cases, if the content is not removed by the content or hosting provider in line with the relevant order, then the only option for the authorities turns out to be access blocking. In other words, at the heart of the problem, there lies the non-compliance of content and hosting providers with the relevant court decisions and the universal principles of the rule of law. Internet governance lays responsibility not only on governments but also on all stake-holder including content and hosting providers. They should act in accordance with professional ethics and comply with the court decisions.

In **Paragraph 49**, it was stated that "*the TIB blocked access to five of the most commonly used LGBTI websites*". The Government would like to reiterate that all blocking access orders are subject to technical and legal supervision under the scope of Law No. 5651 and no special measures have been taken with regard to the "LGBTI" sites, other than those related with child sexual abuse, obscenity and prostitution.

Regarding **Paragraph 50,** the Government would like to set the record straight on the fact that in Turkey there has been no ban decision related to search platforms.

As for removal requests sent to Twitter and Facebook mentioned in **Paragraph 52,** the Government wishes to state that internet actors (content and hosting providers) are expected to develop effective mechanisms in order to solve complaints pertaining to fake accounts, account takeovers, violation of personal rights and/or private life and inappropriate content. Their reluctance to take required measures for user complaints on content that clearly violate even their own policies compel users to apply for related public institutions and legal authorities.

Although it is required to take immediate measures by virtue of a court decision related to such illegal content, these actors frequently continue to broadcast for days. The representatives of the relevant companies have been notified over and over that the courts and related institutions have to step in when user complaints are not solved effectively. Unfortunately, the expected results have not been achieved.

As an addition to information submitted in **Paragraph 54** of the Report, the Government wishes to further elaborate on the nature of application called "Bylock" and the intensive use of this application as a communication tool by the members of the terrorist organization FETÖ/PDY. As specified in the court decisions in Turkey, it is commonly known that this programme is an encrypted communication programme used for secretive illegal communication and organizational contact among the members of the FETÖ/PDY terrorist organization.

In the national court decisions, considerations with regard to the application called Bylock are as follows:

1- ByLock application was put through technical works such as reverse engineering, analysis of encryption, analysis of network behaviour and the codes of the servers connected.

2- It was observed that ByLock application had a design encrypting each message sent with a different encryption in order to ensure the communication with a strong encryption system via Internet connection.

3- The elements supporting the fact that Bylock application was made available for FETÖ/PDY members under the disguise of a global application are as follows;

- There are some "Turkish" expressions in the source codes of the application.
- User names, group names and most of the codes cracked comprise of Turkish expressions.
- Almost all of the contents cracked is in Turkish.
- Although the administrator of the application server claimed that they blocked access to the application with the IP addresses from the Middle East, almost all blocks were aiming at IP addresses from Turkey.
- Those wishing to download the application were obliged to access to it via VPN in order to disguise identities of the users accessing from Turkey and the communication. In addition, almost all the searches about ByLock over "Google" were made by the users from Turkey.
- There has been an increase in "Google" searches about the application as of the date of blocking access to the application with IP addresses from Turkey. Moreover, posts were shared in favour of FETÖ/PDY mostly

through Bylock related online media (social media, web sites, etc.) via fake accounts.

- ***"Bylock", which had a user group more than two hundred thousand, was known by neither Turkish public nor foreign people before the 15th July terrorist coup attempt in Turkey.***

4- It was established that signing up to the application was not sufficient to contact with the users in the system; user names/codes provided mostly face-to-face or by an intermediary (courier, an existing ByLock user etc.) should be added by both sides in order to communicate with each other. It was designed in a way that it will allow to have communication only in accordance with the cell type communication because messaging could be started after both users added each other.

5- Voice call, instant messaging, e-mail delivery and file transfer can be carried out with the application. It was also assessed that organizational communication needs of the users were met by this without needing any other communication tool, and as all the communication was transmitted through the server, groups created and the contents of the communication could be monitored and controlled by the administrator of the application.

6- The correspondence is deleted automatically from the device in specific periods without requiring a manual process. This indicates that the system has been designed in a way that will take the necessary measures even if the users forget to delete the data for the communication security. Therefore it has been established that ByLock application was designed in a way that will prevent to access to the past data of the users and the correspondence if the device is seized as a result of a probable judicial proceeding. In addition, server and communication data of the application is encrypted in the application database and this is regarded as an additional security measure in order to prevent identification of users and ensure the communication security.

7- In order to disguise themselves, the users set a unique and quite long password. For example, there are passwords consisting of about 38 digits among the data, analysis of which have been completed, and more than half of the passwords, analysis of which have been completed, consist of 9 digits and more.

Instead of downloading the application from Android or Apple AppStore after a certain date, the application was uploaded into the devices of users manually. It was also observed that almost all of the messages, which were obtained and analysis of which were completed, included organizational contacts and activities, corresponded to the jargon of the organization.

8- It was understood from the statements of organization members being subject to judicial control proceedings (custody, arrest, apprehension, etc.) after the military coup attempt staged by FETÖ/PDY units on 15 July 2016 that, it was used as an organizational communication tool by the members of FETÖ/PDY organization.

Academic Freedom

With regard to Paragraphs 55-57 on academic freedom, the Government wishes to state that recent measures have been directed towards ensuring and maintaining the academic autonomy of Turkish universities. It is evident that a well-organized illegal terrorist organization such a. FETÖ/PDY is one of the biggest threats to the autonomy of academic institutions and the academic freedom of faculty members. Therefore, it was quite necessary to be persistent in cutting the ties of any illegal organization with Turkish universities.

As for so-called "Peace Petition" mentioned in Paragraph 57, the Government wishes to remind that it has submitted comprehensive information to the UN in response to the Joint Urgent Appeal of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the situation of human rights defenders dated 31 March 2016 (REFERENCE UA, TUR 3/2016).The Government's response is enclosed for perusal and reference.

Certain number of academic staff has been dismissed from their universities as a result of investigations. The expelled academics were proved within the limits of Turkish Law to have close ties with FETÖ/PDY. However, those who have been found innocent are allowed to take their posts back immediately in accordance with the respective Decree Laws numbered 673, 677, 679, 688, 689, and 690. More than a hundred academics have been reinstated to their positions up until today. In addition to executive orders, appeal process is open for the dismissed academic staff as well as other civil servants.

In Paragraph 56 it is stated that "the licences of approximately 21 000 teachers in Gülen operated schools were cancelled". It should be emphasized that the licences of these teachers in private schools were not cancelled just because these persons were working at these schools, but they had worked for FETÖ/PDY. After the cancellations, the situation of teachers who applied by claiming that they were wrongfully suspected were investigated by the Boards formed in provinces and 1.335 teachers licenses were issued back.

Regarding the university elections mentioned in Paragraph 57, it should be emphasized that Turkish constitution grants authority to the President in appointing university rectors since 1981. Today, President of Turkey appoints the rectors upon Council of Higher Education's assessment of the nominees.

Political Activity

As far as the HDP is concerned, the Government wishes to clarify that HDP is not the main opposition party in Turkey as stated in **Paragraph 58**. Main opposition party is another party, namely CHP. Furthermore, in June 2016, the immunity of 154 MPs from ***all political parties*** represented in the parliament including the ruling AK Party was lifted as a result of 810 pending case files before the judicial authorities.

Dismissal of public officials

In **Paragraph 59** it is stated that *"between the time of the attempted coup and the Special Rapporteur's visit, approximately 74,000 public officials had been removed from government positions, and 100,000 had been removed from public office for political, religious or other beliefs. The dismissals take place without trial, investigation or appeal possibilities."*

The Government wishes to reiterate that those individuals are dismissed or suspended not because of political, religious or other beliefs, but due to their membership, affiliation or connection to terrorist organizations and their support to them. No state can accept elements within public institutions that misuse their authority and public resources to realize illegal goals of terrorist organizations.

Measures are taken within the limits of the rule of law and our international obligations. Boards have been established at the office of Prime Minister and the Offices of Governors across Turkey for the people "who believe they have been wrongfully suspected". To date, over 30 thousand employees have been reinstated.

Moreover, with the Decree 685 dated 23 January 2017, an Inquiry Commission on State of Emergency Measures has been established as a binding legal remedy to address measures that are taken directly with Decrees. The Commission will assess applications regarding dismissals of public employees and closure of associations, institutions, as well as media outlets, as listed in relevant Decrees.

This provides an effective domestic legal remedy concerning such cases. The Commission is entitled to take binding decisions with due process. Decisions taken by the Commission are also subject to judicial control. Its decisions can be challenged before relevant courts.

The Commission's members have been recently appointed (16 May 2017) and started its work (22 May 2017). It will soon start to receive applications concerning cases that are listed in relevant Decrees. These revisions demonstrate once again the Government's determination to follow the principles of necessity and proportionality in State of Emergency measures.

Civil Society

In **Paragraph 61**, various claims raised regarding the closure of NGOs in Turkey. The Government would like to remind that there are about 110 thousand associations and 90 thousand foundations currently operating in Turkey. Certain associations were found to be linked with terrorist organizations (FETÖ, PKK, DHKP-C and DAESH) and these were closed with Decree Laws. However, 187 associations and 21 foundations were reopened by Decree Laws. The measures are constantly reviewed and the Inquiry Commission on State

of Emergency measures (see paragraph 36) will also address applications concerning closure of associations and institutions.

In **Paragraph 66** of the Report, it was alleged that *"the judiciary appeared to be unreasonably unavailable to the tens of thousands of individuals who had lost their employment according to vague accusations of association with the Gülenist movement and Kurdish organizations"*.

Article 148 of the Turkish Constitution provides that decrees having the force of law issued during a State of Emergency shall not be brought before the Constitutional Court

alleging their unconstitutionality as to form or substance and in accordance with Article 121 of the Constitution, Decree Laws are submitted to the Grand National Assembly of Turkey for approval on the day they have been published in the Official Gazette. Nevertheless, judicial review is possible in respect of measures by public institutions which have been introduced based on the procedure laid down in Decree Laws. Since such measures based on the powers conferred by Decree Laws are open to judicial review, individual applications are also possible against these measures.

However, as the dismissals made directly through Decree Laws technically have the nature of legislative activities, filing objections or making individual applications against these measures were not possible until the adoption of the Decree-Law no. 685. With the adoption of the Decree-Law no. 685 on January 23, 2017, the Inquiry Commission on State of Emergency Measures was introduced to examine and conclude applications related to dismissals from profession, removal from studentship, closure of institutions and organizations, and deprivation of ranks from retired officials on grounds of membership, affiliation or connection to terrorist organizations, when imposed directly through decree laws. This Commission is entitled to take binding decisions with due process. Decisions taken by this Commission are also subject to judicial control. Its decisions can be challenged before relevant courts.

As mentioned before, the Commission's Members have been recently appointed (16 May). It will soon start to receive applications concerning cases that are listed in relevant Decrees. Upon a decision of reinstatement by the Commission, the State Personnel Department shall reappoint the official concerned, reserving his/her vested rights. Those who had been removed from executive positions shall be appointed in line with their previous posts. Moreover, any party claiming that the Commission's decision violates their interests shall be able to file an action with administrative courts for the annulment of these decisions.

By the Decree-Law no. 667, members of the judiciary who were dismissed from profession by the Board of Judges and Prosecutors (HSK) and by higher courts, are entitled to file an action directly with the Council of State. These provisions shall apply to those who had previously filed actions or even for those about whom decisions have already been taken.

By the Decree-Law no. 685, effective domestic remedies have been introduced in respect of measures imposed or to be imposed by State of Emergency Decree Laws.

Structural changes to judiciary

In **Paragraph 68** of the Report, concerns were raised as to the independence of the judiciary, followed by comments on the establishment of criminal magistrate's offices and the relevant appeal procedure.

The Government wishes to underline that by the promulgation of the Law no. 6545, amending the Penal Code, on 18 June 2014, among others, Criminal Courts of Peace were revoked and replaced by Criminal Magistrate's Offices, entrusted with taking the necessary decisions within the purview of judges in all investigations conducted, carrying out relevant duties and examining the objections made against these decisions. The establishment of Criminal Magistrate's Offices was aimed at ensuring specialisation on investigatory proceedings and uniform practice, and gradually achieving nationwide standards in the decisions taken regarding protective measures.

In terms of appointment and function, criminal magistrates are not different from other criminal court judges. They are appointed by the HSK, which has administrative and financial independence under Article 159 of the Constitution, in accordance with the guarantees of "independence and impartiality of judges". The Constitutional Court has examined, both as a response to an individual petition and through the review of norms, the institution of criminal magistracy. The court decided that criminal magistrates, not dissimilar to other judges, were appointed by the HSK and they possessed the security of tenure envisaged in the Constitution. The Constitutional Court ruled that there was no reason to suggest that these magistrates were in a different position than other judges and that safeguards for their independence were compromised (see no. 2014/164 E, 2014/112 K, review of norms, and *Hikmet Kaşar and Others* (individual application, no. 2014/4494)).

The legislator has envisaged that appeals against the decisions by Magistrate's Offices, which were established as a specialisation authority for decisions at the investigation stage, shall also be concluded by these Magistrates. This conclusion is in line with the legislator's intention to separate the proceedings at the investigative stage from that of the prosecution stage. Moreover, it serves to ensure specialisation and uniformity. In accordance with the Article 267 of the Law No.5271, decisions of the criminal magistrate's offices are subject to objection and a procedure is available for the effective supervision of decisions taken in investigative stage regarding the protective safeguards.

Although it is a matter of criticism that appeals to decisions by Magistrate's Offices shall also be reviewed by the same authority, the rule should not be considered incompatible with the ECHR principles taking into account the following reasons:

Criminal Magistrate's Offices have no duties at the trial stage;

They are not empowered to give a final verdict in respect of suspects or defendants; and

The decisions of protective nature they may take during the investigation stage come under review by the trial court following the approval of the bill of indictment.

The appeal review is not a mutual examination of one Magistrate's decision by another but appeals are submitted to the next or closest criminal magistrate.

Like other judges, Criminal Magistrates are appointed by the HSK with regard to their career features, competence and merit. There are no elements in the establishment or functioning of these posts which lead to the conclusion that they may not serve with impartiality. However, if it can be demonstrated by concrete, objective and convincing

proof that a judge has lost his/her impartiality, he/she can be removed from conducting the trial in line with procedural law.

As one can observe from the judgments of the Constitutional Court and similar case-law of the ECHR, with regard to their appointment procedures, duties, competence and work procedures, criminal magistrate's offices have been established and have been serving in line with the principles of natural justice and independence/impartiality.

Dismissals of judges and prosecutors

In **Paragraph 70**, it was falsely asserted that *judges and prosecutors were removed "under emergency decree"*. The truth is, although many public officials were dismissed by the inclusion of their names in the lists annexed to emergency decrees, judges and prosecutors are actually dismissed from profession by decisions taken by the General Assembly of the HSK.

HSK is the authority to take decisions on removing judges and prosecutors from office who were found to have membership, affiliation, connection or links to terrorist organizations. A long-standing administrative inquiry has identified these persons as being members of the FETÖ/PDY, and an investigation was initiated *ex officio* under Article 161/6 of the Code of Criminal Procedure and detention orders were taken by the Ankara Chief Public Prosecutor's Office. These circumstances have been taken into account and the judges and prosecutors who were found to have membership, affiliation, connection or links to terrorist organizations were dismissed by the General Assembly of the HSK.

As mentioned before, by the Decree-Law no. 667, members of the judiciary who were dismissed from profession by the Board of Judges and Prosecutors (HSK) and by higher courts, are entitled to file an action directly with the Supreme Administrative Court. These provisions shall apply to those who had previously filed actions or even for those about whom decisions have already been taken.

Lack of judicial review

As to the reference in **Paragraph 71** of the Report to the decision of 12 October 2016 by the Turkish Constitutional Court, the Government wishes to elaborate that this was a decision regarding the Decree Laws no. 668 and 669, which were examined within the context of review of norms by the Court. The Court ruled that a judicial review of the merits was not possible, referring to the provision in Article 148/1 of the Constitution, which reads "... decrees having the force of law issued during a State of Emergency, martial law or in time of war shall not be brought before the Constitutional Court alleging their unconstitutionality as to form or substance". Therefore, the Constitutional Court rejected requests for the annulment of Decree Laws for lack of jurisdiction.

Contrary to the comment in the Report, it is evident that the Constitutional Court's decision of 12 October 2016 was a response to the request for the annulment of the Decrees Laws no. 668 and 669 through a review of norms, which is irrelevant to individual applications. The Constitutional Court has rejected the application based on the clear legal rule under Article 148 of the Constitution, due to lack of jurisdiction. However, no rule has been contained in the said provision regarding individual applications. Therefore, a generic interpretation of this decision of the Court to reach conclusions on individual applications is not appropriate.

Access to lawyer and due process

Paragraph 72 of the Report reads as follows :

Emergency decree 667, the first declared following the attempted coup, increased the amount of time a detainee could be held without charge from four to thirty days (article 6a). Article 19 of the Constitution allows for a maximum of four days and an extension of

this period during a state of emergency. However, in the case of Aksoy v. Turkey, the ECtHR held that detention of fourteen days without judicial review, even during a legitimate state of emergency, violated the state's human rights obligations.

The Government wishes to inform that pursuant to the Decree Laws no. 667 and 668 and the Laws no. 6749 and 6755 which are the approved form of these decrees, the duration of police custody had been extended to a maximum of 30 days during the emergency period, in respect of terror-related, attempted coup and collective offenses. The following procedural safeguards are available during police custody:

- An objection can be made against the detention order;
- Release can always be requested during police custody;
- Assistance of a lawyer is available;
- Medical reports are always obtained upon taking into and release from custody.

It has been laid down in a later Decree Law no. 684 that this detention period was shortened not to exceed seven days from arrest, excluding the time spent to take the suspect to the nearest court. However, this period can be extended for up to another seven days in writing due to compelling circumstances such as hardships in evidence collection and the large number of suspects. As can be seen, as a result of a risk assessment, the 30-day maximum detention period was reduced to seven days. This new arrangement complies with the judgments of *Aksoy v. Turkey* and *Lawless v. UK* by the ECtHR.

Furthermore, these detention periods are applicable only in respect of terror-related, attempted coup and collective offenses and detention periods for other offences are 1 day and can be extended for up to 4 days only.

The Report only refers to the provisions of the Decree-Law no. 667, a part of which have been revoked. However, there is no mention of the provisions introduced by the Decree-Law no. 684, which are now in force.

Enc. 2

United Nations A/HRC/35/22/Add.7

General Assembly

Distr.: General
9 June 2017

English only

Human Rights Council
Thirty-fifth session
6-23 June 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, socizl and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Tajikistan: comments by the State

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the comments by the State on the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Tajikistan.

GE.17-09482(E)
1709482

Please recycle

Report of the Special Rapporteur the promotion and protection of the right to freedom of opinion and expression on his mission to Tajikistan: comments by the State*

Response to recommendations

Summing up the report, the Government of Tajikistan considers it for necessary to note that the arguments and conclusions made in the report of the SR have been prepared without taking into account the specifics of the country's legislation, Tajikistan's international obligations in the field of human rights, the country's striving to ensure transparency of activities of political parties and public associations, combating terrorism and extremism, as well as its endeavors to counteract money laundering which is often used for financing of terrorism.

The presented document constitutes the speculations of the SR, since it contains such word constructions as "apparently", "as I was told", "there could be pressure", and the conclusions made on individual issues are not supported by concrete facts and examples.

It should be noted that during his visit, Mr. Kaye held a number of meetings with the heads of ministries and departments of the country, but the report does not mention the results of the meetings held, as well as the achievements of the country in the promotion and protection of the right to freedom of expression and opinion. While drafting the report, the comments submitted by the heads of relevant governmental structures on certain issues raised by the SR have been ignored.

For example, during the meeting with the Minister of Justice, the SR was provided with information on national legislation on the right of citizens to freedom of opinion and expression, as well as the activities of public associations and political parties, and on the right of citizens to hold demonstrations.

Also, the SR was explained in detail the reasons for introducing amendments to the Law of the Republic of Tajikistan "On Public Associations" which were implemented in accordance with recommendations of the Financial Action Task Force on Money Laundering (FATF) and the UN Convention against Corruption.

However, the report does not include this information and the comments submitted by the Minister of Justice, but only interprets the situation from the point of view of the representatives of civil society, which by itself makes this report unilateral and biased.

It should be recalled that the powers of the UN SR are limited in the framework of the UN Human Rights Council Resolution 7/36, paragraph 6 of the UN General Assembly Resolution 60/251 from 15 March 2006, as well as the Code of Conduct for Special Procedures Mandates of the UN Human Rights Council.

These documents provide for the terms of reference of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which include the application of efforts to promote and protect the right to freedom of opinion and expression; development of cooperation with UN treaty bodies; presentation of the views on problems in the field of information and communication technologies, including the Internet and mobile communications; integration of women's rights and the gender dimension in the work to fulfill their mandate; requesting reliable and truthful information from governments, non-governmental organizations and any other parties and responding to it; preparation of the recommendations and proposals on ways and means for improvement of promotion and protection of the right to freedom of opinion and expression etc.

---

* Reproduced as received.

However, the issues raised by the SR during the preparation of the report, such as ban of the Islamic Renaissance Party of Tajikistan, the introduction of amendments and additions to the Law of the Republic of Tajikistan "On Public Associations", the introduction of amendments to the Constitution and many other issues go beyond his mandate determined by the resolutions of the UN Human Rights Council and the UN General Assembly.

It should be underlined that due to the adopted mandate, the SR should establish a constructive dialogue with states and work on the basis of principles of impartiality, integrity and objectivity.

The Government considers the information presented in the report as biased and one-sided, based only on the information of some representatives of non-governmental organizations. This attitude of the SR at least gives rise to doubts about his impartiality and objectivity.

It is crucial to take into account the positions and opinions of both non-governmental and governmental sides in order to refrain from unilateral interpretation of issues, and proceed from the provisions of current national legislation, international obligations of the country in the field of human rights and actual situation within the country and in regional and global contexts.